EXPERTENSESSION

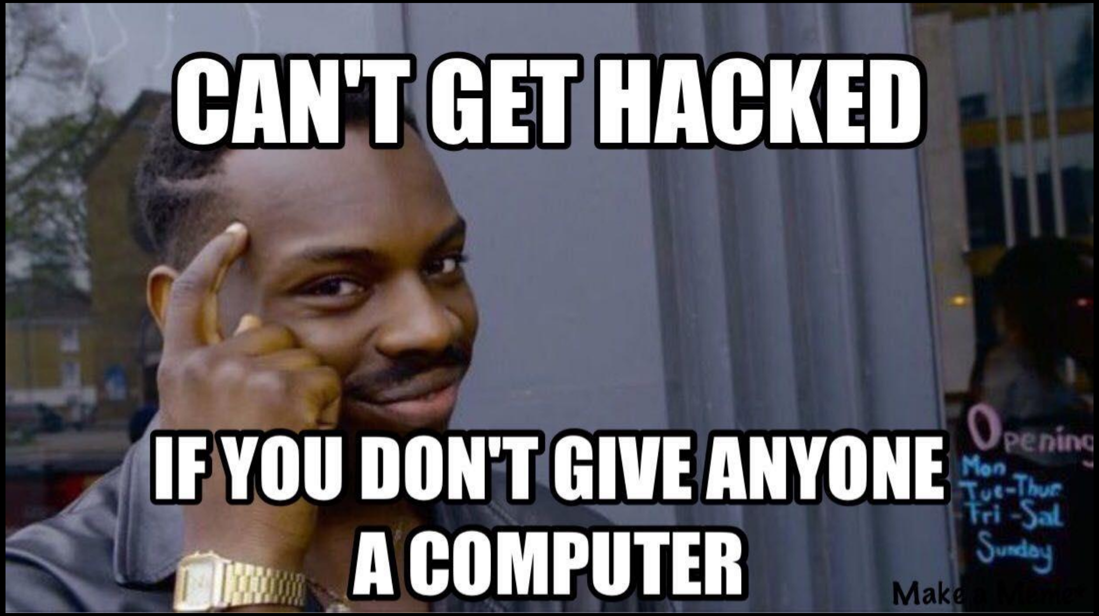
Wirksamer Umgang mit OT Cyber-Risiken

CyberCompare
A BOSCH BUSINESS

Oliver Herterich

DRAGOS

5 Critical Controls



5 Critical Controls

A Threat focused approach for the OT Cybersecurity Strategy

DETECT

Understand adversary threats targeting your industry

RESPOND

TTPs to more effectively hunt & reduce dwell time

RECOVER

Faster investigations & effective vulnerability management

Preparation

Preparation

A Threat based approach for the OT Cybersecurity Strategy

What are you defending against?

- Research previous attacks
- Define the 3-5 real-world scenarios
- Explain the difference between IT and OT

Build the foundation with executive alignment

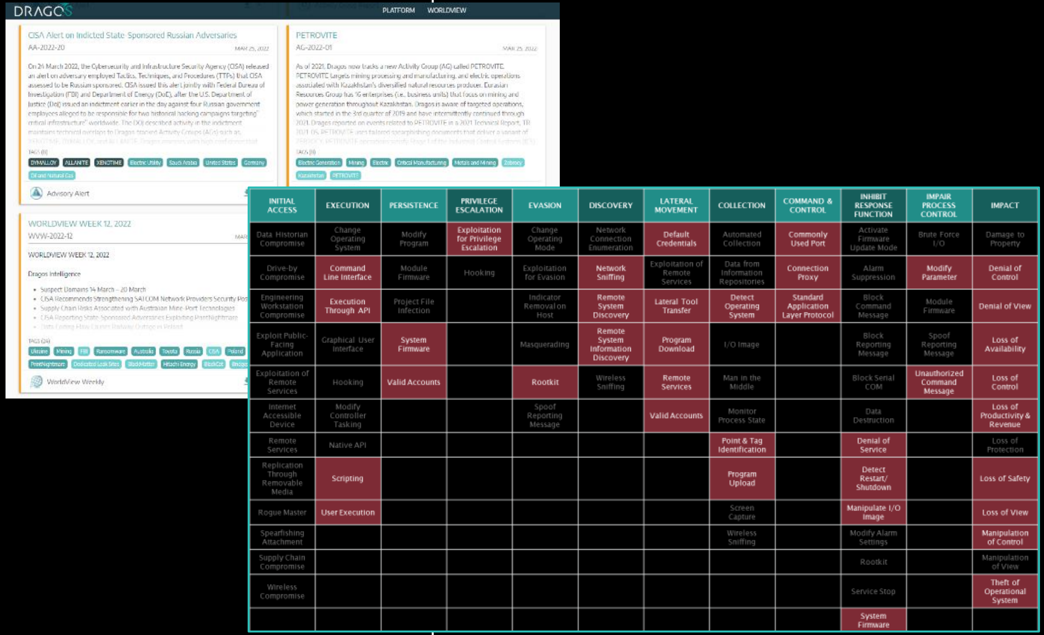
- Top-down approach

Prioritization

- most important sites in the company
- systems and locations to focus on first

Collaboration between IT and OT

- Define technology that can be shared/aligned



CISA Alert on Indicted State-Sponsored Russian Adversaries
AA-2022-20
MAR 25, 2022

On 24 March 2022, the Cybersecurity and Infrastructure Security Agency (CISA) released an alert on adversary employed Tactics, Techniques, and Procedures (TTPs) that CISA assessed to be Russian sponsored. CISA issued this alert jointly with Federal Bureau of Investigation (FBI) and Department of Energy (DoE), after the U.S. Department of Justice (DoJ) issued an indictment earlier in the day against four Russian government employees alleged to be responsible for two historical hacking campaigns targeting "critical infrastructure" worldwide. The DOJ described activity in the indictment maintains technical overlaps to Dragos-tracked Activity Groups (AGs) such as XENOTIME, DYMALLOY, and ALLANITE. Dragos assesses with high confidence that

TAGS (8)
DYMALLOY · ALLANITE · XENOTIME · Electric Utility · Saudi Arabia · United States · Germany · Oil and Natural Gas

Advisory Alert

PETROVITE
AG-2022-01
MAR 25, 2022

As of 2021, Dragos now tracks a new Activity Group (AG) called PETROVITE. PETROVITE targets mining processing and manufacturing, and electric operations associated with Kazakhstan's diversified natural resources producer. Eurasian Resources Group has 16 enterprises (i.e., business units) that focus on mining and power generation throughout Kazakhstan. Dragos is aware of targeted operations, which started in the 3rd quarter of 2019 and have intermittently continued through 2021. Dragos reported on events related to PETROVITE in a 2021 Technical Report, TR-2021-05. PETROVITE uses tailored spearphishing documents that deliver a variant of ZEBROCY. PETROVITE operations satisfy Stage 1 of the Industrial Control Systems (ICS)

TAGS (8)
Electric Generation · Mining · Electric · Critical Manufacturing · Metals and Mining · Zebrocy · Kazakhstan · PETROVITE

WORLDVIEW WEEK 12, 2022
WVW-2022-12
MAR

WORLDVIEW WEEK 12, 2022

Dragos Intelligence

- Suspect Domains 14 March – 20 March
- CISA Recommends Strengthening SATCOM Network Providers Security Pos
- Supply Chain Risks Associated with Australian Mine-Port Technologies
- CISA Reporting State-Sponsored Adversaries Exploiting PrintNightmare
- Data Exiting Flaw Causes Railway Outage in Poland

TAGS (24)
Ukraine · Mining · FBI · Ransomware · Australia · Toyota · Russia · CISA · Poland · PrintNightmare · Dedicated Leak Sites · BlackMatter · Hitachi Energy · BlackCat · Bridges

WorldView Weekly

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating System	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution Through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating System	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Internet Accessible Device	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity & Revenue
Remote Services	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Replication Through Removable Media	Scripting						Program Upload		Detect Restart/ Shutdown		Loss of Safety
Rogue Master	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Spearfishing Attachment							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Supply Chain Compromise									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational System
									System Firmware		

ICS INCIDENT RESPONSE PLAN

1 ICS INCIDENT RESPONSE PLAN

IT vs. OT

System & Data vs. System of Systems and physics

OT's incident and response plan is distinct from IT's.

Different

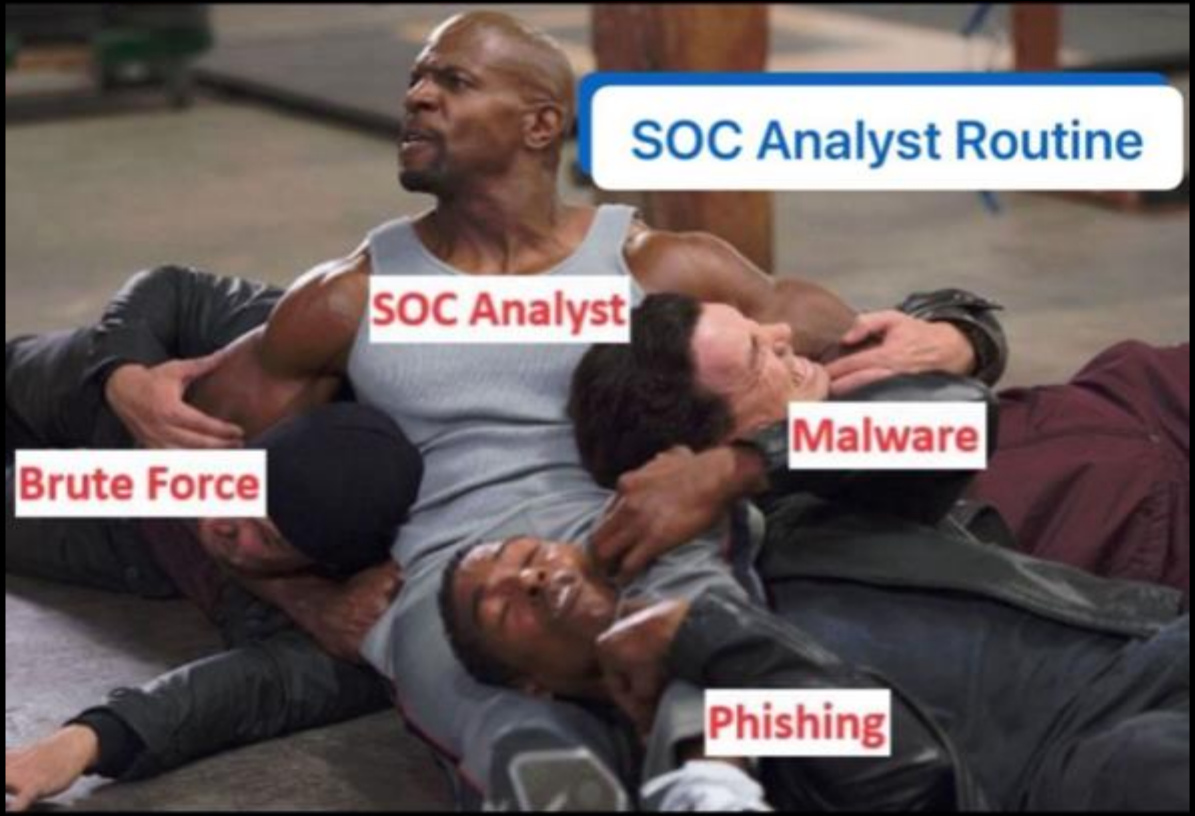
Device types	Communication protocols
Tactics	Techniques and procedures

Managing the potential impact of an incident is different for OT.

Create a dedicated plan and next steps for specific scenarios

2

DEFENSIBLE ARCHITECTURE



2 DEFENSIBLE ARCHITECTURE

CyberCompare
A BOSCH BUSINESS

The resources and technical skills required to adapt to new vulnerabilities and threats should not be underestimated.

Removing extraneous OT network access points

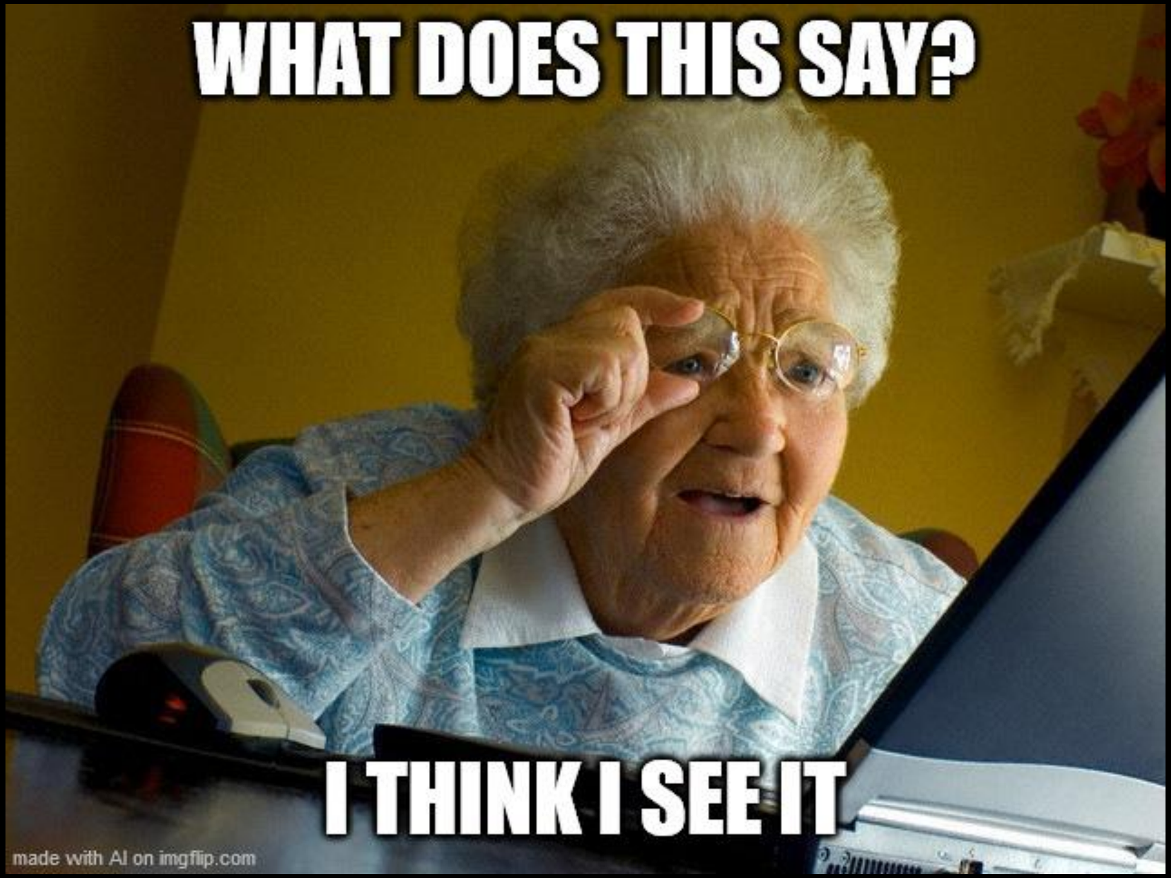
Mitigating high risk vulnerabilities

Maintaining strong policy control at IT/OT interface points

The people and processes to maintain it

DRAGOS

3 OT VISIBILITY & MONITORING



3 OT VISIBILITY & MONITORING

You can't protect
what you can't see.

IN 2022
80%
of Dragos services customers had limited to no visibility in their OT environments

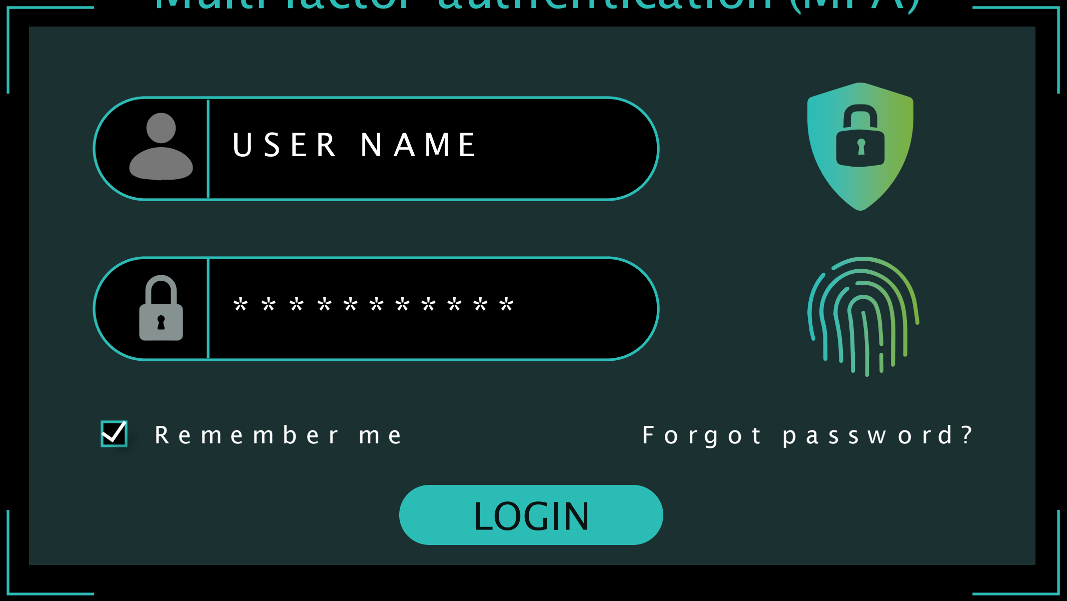
A Successful
OT Security Posture

- ✓ Maintains an inventory of assets
- ✓ Maps vulnerabilities against those assets
- ✓ Actively monitors traffic for potential threats
- ✓ validating the security controls implemented in a defensible architecture

4 SECURE REMOTE ACCESS / MFA

4 SECURE REMOTE ACCESS / MFA

Multi-factor authentication (MFA)



MFA Is a rare case of a classic IT control that can be appropriately applied to OT.

Implement MFA across your systems of systems to add an **extra layer of security** for a relatively small investment.

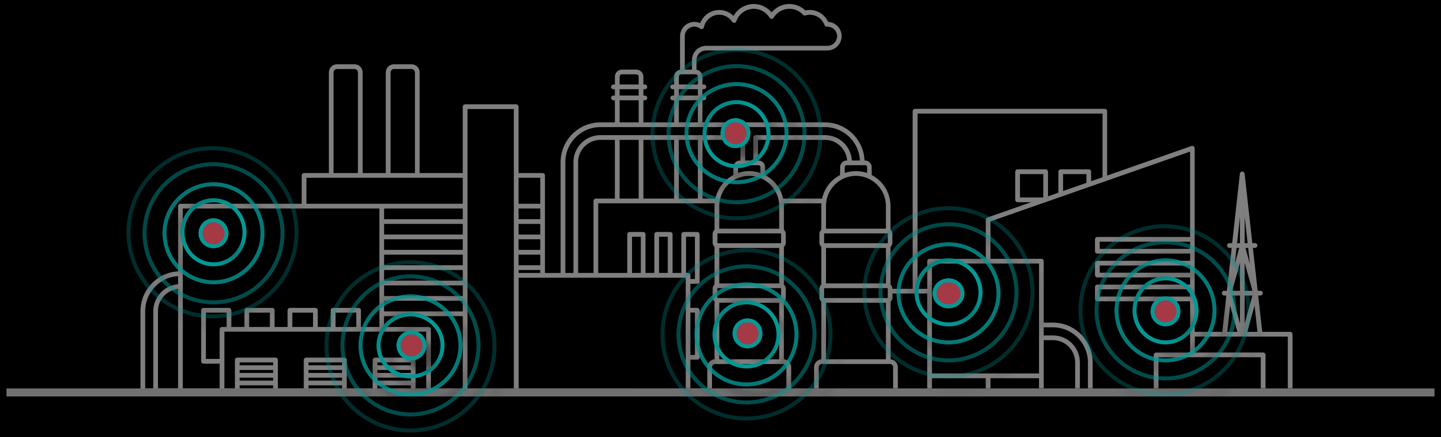
5

RISK-BASED VULNERABILITY MANAGEMENT

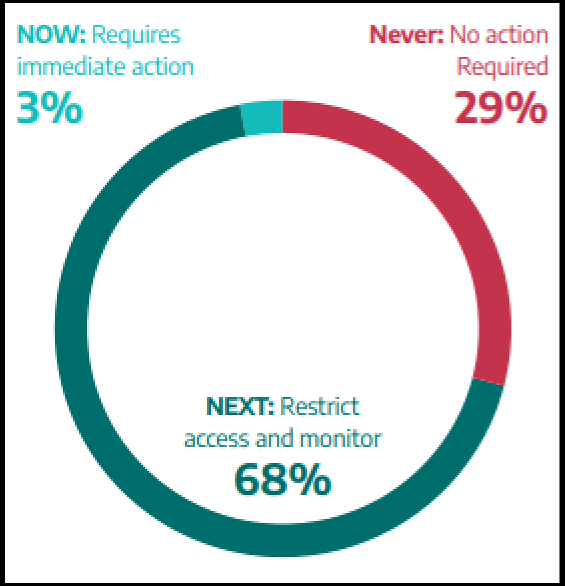
CyberCompare
A BOSCH BUSINESS

5 RISK-BASED VULNERABILITY MANAGEMENT

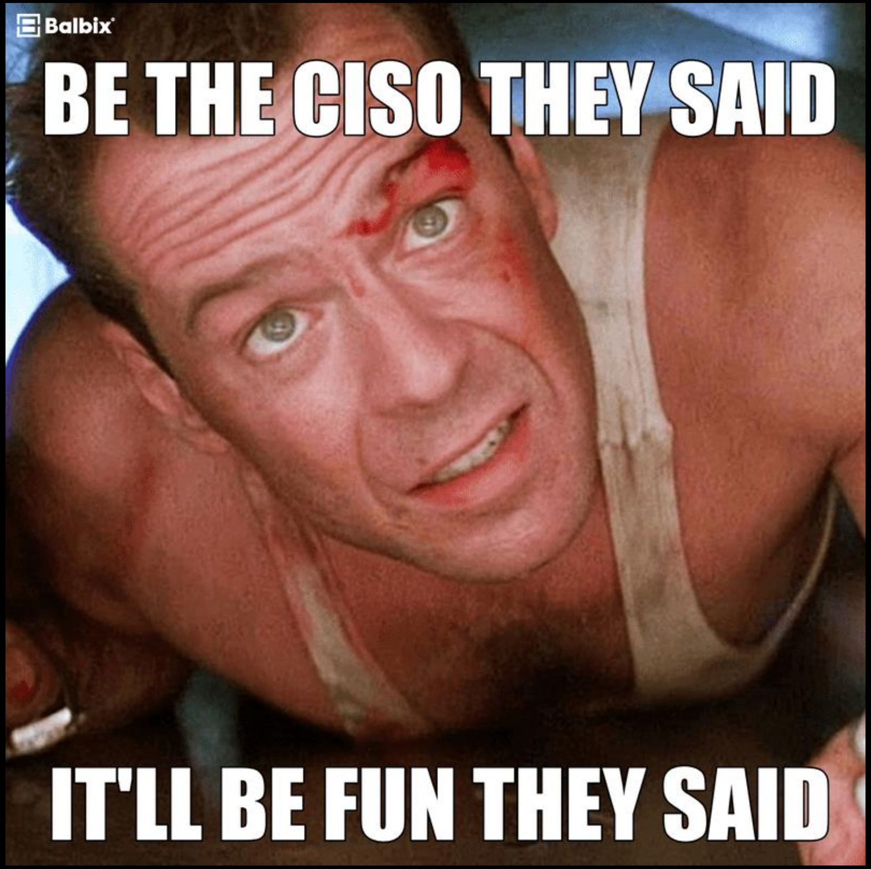
CyberCompare
A BOSCH BUSINESS



Knowing your vulnerabilities
and having a plan to manage them is a critical component to a defensible architecture.



OT CYBERSECURITY STRATEGY



OT CYBERSECURITY STRATEGY

CRITICAL CONTROLS FOR EFFECTIVE OT CYBERSECURITY

The right controls to ensure world-class OT cybersecurity

01
An ICS incident response plan

02
A defensible architecture

03
OT visibility and monitoring

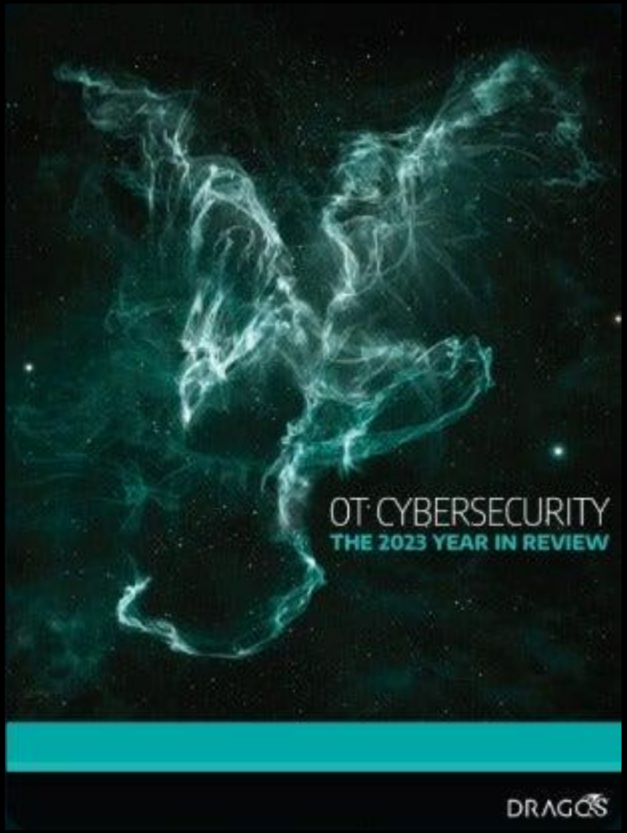
04
Secure remote access / MFA

05
Risk-based vulnerability management

THANK YOU

Oliver Herterich
Senior Solution Architect DACH & EE

oherterich@dragos.com
O: +49 175 419 1079



Ressources:

Dragos Year in Review 2023:
https://www.dragos.com/ot-cybersecurity-year-in-review/#anchor-report

SANS Whitepaper – 5 Critical Controls:
https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

EXPERTENSESSION

Praxisbeispiel: Umsetzung eines OT-Cybersicherheitsprogramms

CyberCompare
A BOSCH BUSINESS

Oliver Herterich

DRAGOS

OT CYBERSECURITY STRATEGY

CRITICAL CONTROLS FOR EFFECTIVE OT CYBERSECURITY

The right controls to ensure world-class OT cybersecurity

01
An ICS incident response plan

02
A defensible architecture

03
OT visibility and monitoring

04
Secure remote access / MFA

05
Risk-based vulnerability management

Customer

CyberCompare
A BOSCH BUSINESS

Situation

- ONG customer
- Distributed locations
- Lack of dedicated security resources
- Lack of an OT incident response plan
- No Safety system segmentation
- No offline/offsite backups
- …

Preparation

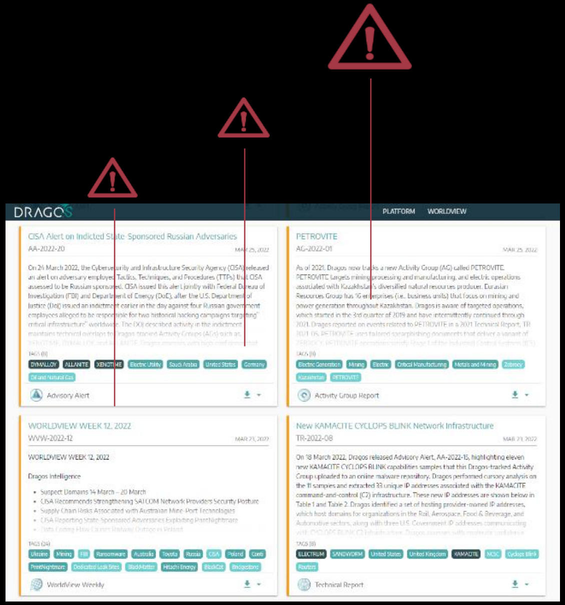
A Threat based approach for the OT Cybersecurity Strategy

What are you defending against? OT-focused intelligence reporting

- Ransomware
- Trisis malware
- Pipedream malware

Build the foundation with executive alignment

- Top-down approach



DRAGOS PLATFORM WORLDVIEW

CISA Alert on Indicted State-Sponsored Russian Adversaries
AA-2022-20 MAR 25, 2022

On 24 March 2022, the Cybersecurity and Infrastructure Security Agency (CISA) released an alert on adversary employed Tactics, Techniques, and Procedures (TTPs) that CISA assessed to be Russian sponsored. CISA issued this alert jointly with Federal Bureau of Investigation (FBI) and Department of Energy (DoE), after the U.S. Department of Justice (DoJ) issued an indictment earlier in the day against four Russian government employees alleged to be responsible for two historical hacking campaigns targeting "critical infrastructure" worldwide. The DOJ described activity in the indictment maintains technical overlaps to Dragos-tracked Activity Groups (AGs) such as XENOTIME, DYMALLOY, and ALLANITE. Dragos assesses with high confidence that

TAGS (8)
DYMALLOY ALLANITE XENOTIME Electric Utility Saudi Arabia United States Germany Oil and Natural Gas

Advisory Alert

PETROVITE
AG-2022-01 MAR 25, 2022

As of 2021, Dragos now tracks a new Activity Group (AG) called PETROVITE. PETROVITE targets mining processing and manufacturing, and electric operations associated with Kazakhstan's diversified natural resources producer, Eurasian Resources Group has 16 enterprises (i.e., business units) that focus on mining and power generation throughout Kazakhstan. Dragos is aware of targeted operations, which started in the 3rd quarter of 2019 and have intermittently continued through 2021. Dragos reported on events related to PETROVITE in a 2021 Technical Report, TR 2021-05. PETROVITE uses tailored spearphishing documents that deliver a variant of [illegible]

TAGS (8)
Electric Generation Mining Electric Critical Manufacturing Metals and Mining Zebrocy Kazakhstan PETROVITE

Activity Group Report

WORLDVIEW WEEK 12, 2022
WVW-2022-12 MAR 23, 2022

WORLDVIEW WEEK 12, 2022

Dragos Intelligence

- Suspect Domains 14 March – 20 March
- CISA Recommends Strengthening SATCOM Network Providers Security Posture
- Supply Chain Risks Associated with Australian Mine-Port Technologies
- CISA Reporting State-Sponsored Adversaries Exploiting PrintNightmare
- Data Coming Flaw Causes Railway Outage in Poland

TAGS (24)
Ukraine Mining FBI Ransomware Australia Toyota Russia CISA Poland Conti PrintNightmare Dedicated Leak Sites BlackMatter Hitachi Energy BlackCat Bridgestone

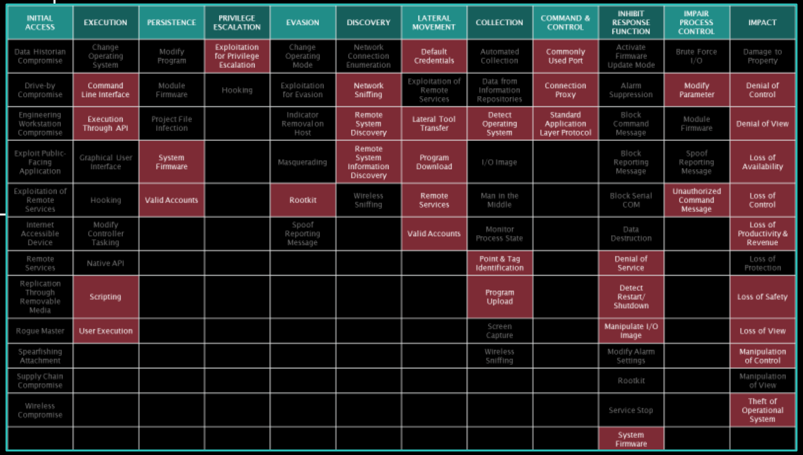
WorldView Weekly

New KAMACITE CYCLOPS BLINK Network Infrastructure
TR-2022-08 MAR 23, 2022

On 18 March 2022, Dragos released Advisory Alert, AA-2022-15, highlighting eleven new KAMACITE CYCLOPS BLINK capabilities samples that this Dragos-tracked Activity Group uploaded to an online malware repository. Dragos performed cursory analysis on the 11 samples and extracted 33 unique IP addresses associated with the KAMACITE command-and-control (C2) infrastructure. These new IP addresses are shown below in Table 1 and Table 2. Dragos identified a set of hosting provider-owned IP addresses, which host domains for organizations in the Rail, Aerospace, Food & Beverage, and Automotive sectors, along with three U.S. Government IP addresses communicating with CYCLOPS BLINK C2 infrastructure. Dragos assesses with moderate confidence

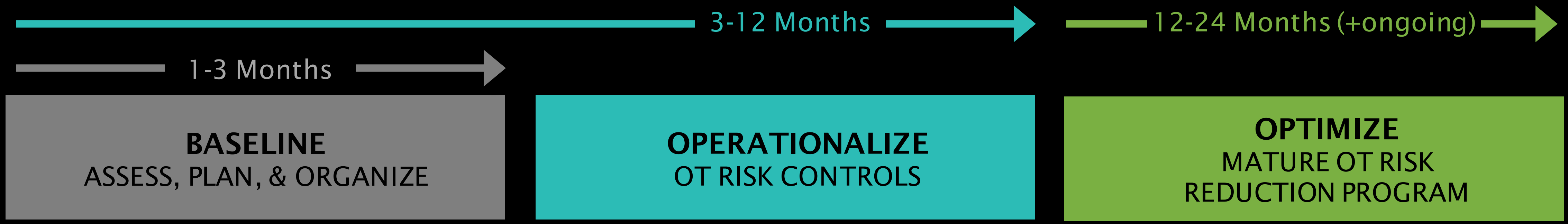
TAGS (8)
ELECTRUM SANDWORM United States United Kingdom KAMACITE NCSC Cyclops Blink Routers

Technical Report



INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating System	Modify Program	**Exploitation for Privilege Escalation**	Change Operating Mode	Network Connection Enumeration	**Default Credentials**	Automated Collection	**Commonly Used Port**	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	**Command Line Interface**	Module Firmware	Hooking	Exploitation for Evasion	**Network Sniffing**	Exploitation of Remote Services	Data from Information Repositories	**Connection Proxy**	Alarm Suppression	**Modify Parameter**	**Denial of Control**
Engineering Workstation Compromise	**Execution Through API**	Project File Infection		Indicator Removal on Host	**Remote System Discovery**	**Lateral Tool Transfer**	**Detect Operating System**	**Standard Application Layer Protocol**	Block Command Message	Module Firmware	**Denial of View**
Exploit Public-Facing Application	Graphical User Interface	**System Firmware**		Masquerading	**Remote System Information Discovery**	**Program Download**	I/O Image		Block Reporting Message	Spoof Reporting Message	**Loss of Availability**
Exploitation of Remote Services	Hooking	**Valid Accounts**		**Rootkit**	Wireless Sniffing	**Remote Services**	Man in the Middle		Block Serial COM	**Unauthorized Command Message**	**Loss of Control**
Internet Accessible Device	Modify Controller Tasking			Spoof Reporting Message		**Valid Accounts**	Monitor Process State		Data Destruction		**Loss of Productivity & Revenue**
Remote Services	Native API						**Point & Tag Identification**		**Denial of Service**		Loss of Protection
Replication Through Removable Media	**Scripting**						**Program Upload**		**Detect Restart/ Shutdown**		**Loss of Safety**
Rogue Master	**User Execution**						Screen Capture		**Manipulate I/O Image**		**Loss of View**
Spearfishing Attachment							Wireless Sniffing		Modify Alarm Settings		**Manipulation of Control**
Supply Chain Compromise									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		**Theft of Operational System**
									System Firmware		

ICS/OT Cyber Security Journey



1-3 Months

3-12 Months

12-24 Months (+ongoing)

BASELINE
ASSESS, PLAN, & ORGANIZE

OPERATIONALIZE
OT RISK CONTROLS

OPTIMIZE
MATURE OT RISK REDUCTION PROGRAM

Establish Baseline
(leverage Dragos Platform)

- Conduct Architecture Assessment
- Create an Incident Response Plan
- Organize your assets inventory & collection management framework
- Define Threat Scenarios

Operate Dragos Platform

- Monitor OT assets & network traffic in Crown Jewel sites
- Identify & manage key OT vulnerabilities
- Detect & respond to OT incidents

Expand & Mature

- Expand deployment to medium & low impact OT sites
- Integrate OT incidents & intelligence with IT SOC
- Validate defensive controls

1 ICS INCIDENT RESPONSE PLAN

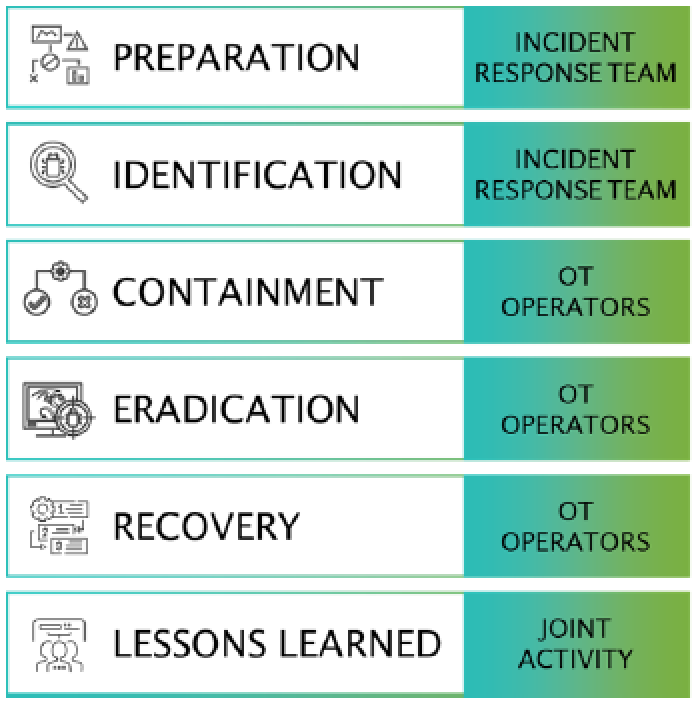
1) Develop **ICS Incident Response Plan**

2) Establish **Dragos Incident Response Retainer**

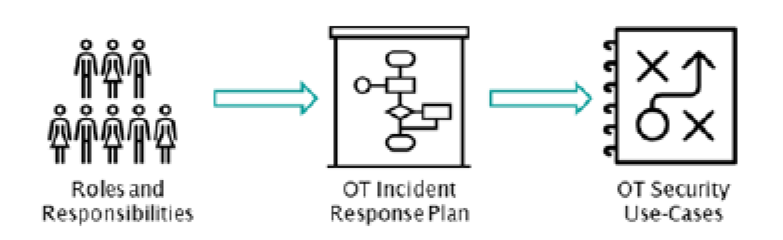
3) Define **Roles and Responsibilities**

4) **OT-SOC Establishment** Plan

5) Recurring **Tabletop Exercises** and refinement of IRP



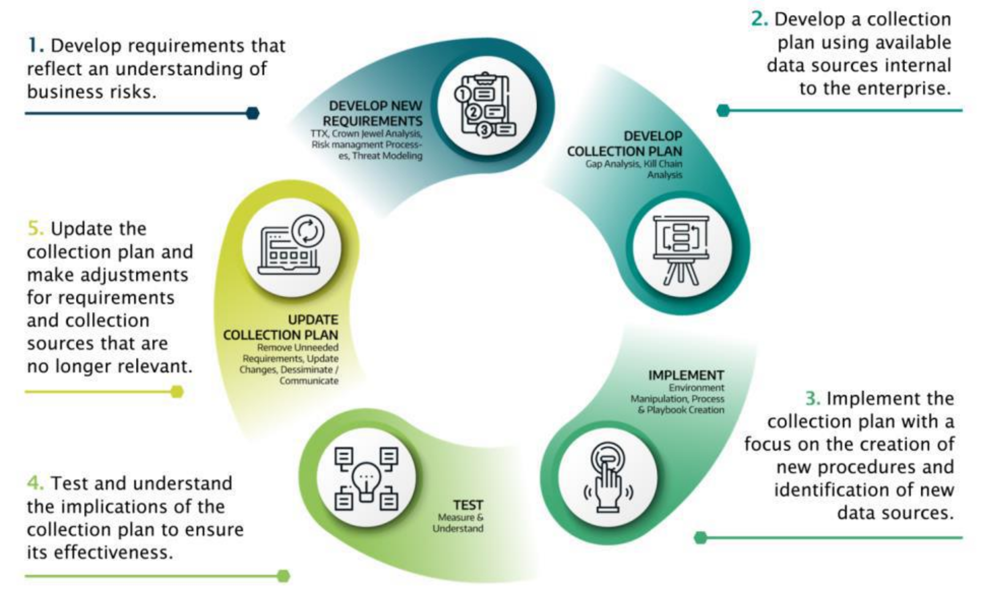
PREPARATION	INCIDENT RESPONSE TEAM
IDENTIFICATION	INCIDENT RESPONSE TEAM
CONTAINMENT	OT OPERATORS
ERADICATION	OT OPERATORS
RECOVERY	OT OPERATORS
LESSONS LEARNED	JOINT ACTIVITY



1 ICS INCIDENT RESPONSE PLAN

Collection Management Framework (CMF)

is a process that documents and institutionalizes data sources that are available to defenders, including what information is available, where that data lives, how it is accessed, and how long that data is retained



1. Develop requirements that reflect an understanding of business risks.

2. Develop a collection plan using available data sources internal to the enterprise.

3. Implement the collection plan with a focus on the creation of new procedures and identification of new data sources.

4. Test and understand the implications of the collection plan to ensure its effectiveness.

5. Update the collection plan and make adjustments for requirements and collection sources that are no longer relevant.

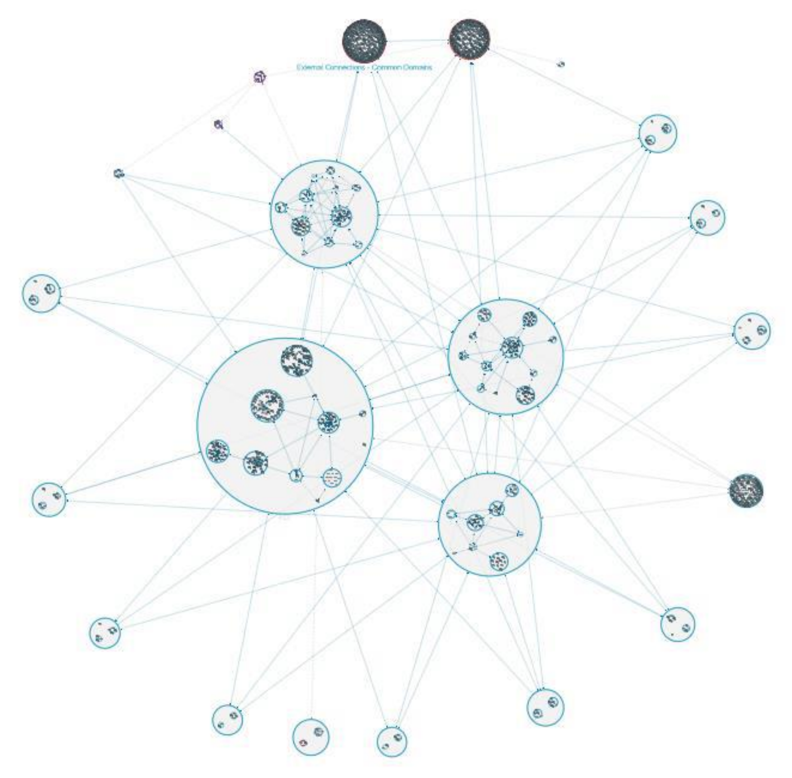
DEVELOP NEW REQUIREMENTS
TTX, Crown Jewel Analysis, Risk managment Process-es, Threat Modeling
DEVELOP COLLECTION PLAN
Gap Analysis, Kill Chain Analysis
IMPLEMENT
Environment Manipulation, Process & Playbook Creation
TEST
Measure & Understand
UPDATE COLLECTION PLAN
Remove Unneeded Requirements, Update Changes, Dessiminate / Communicate

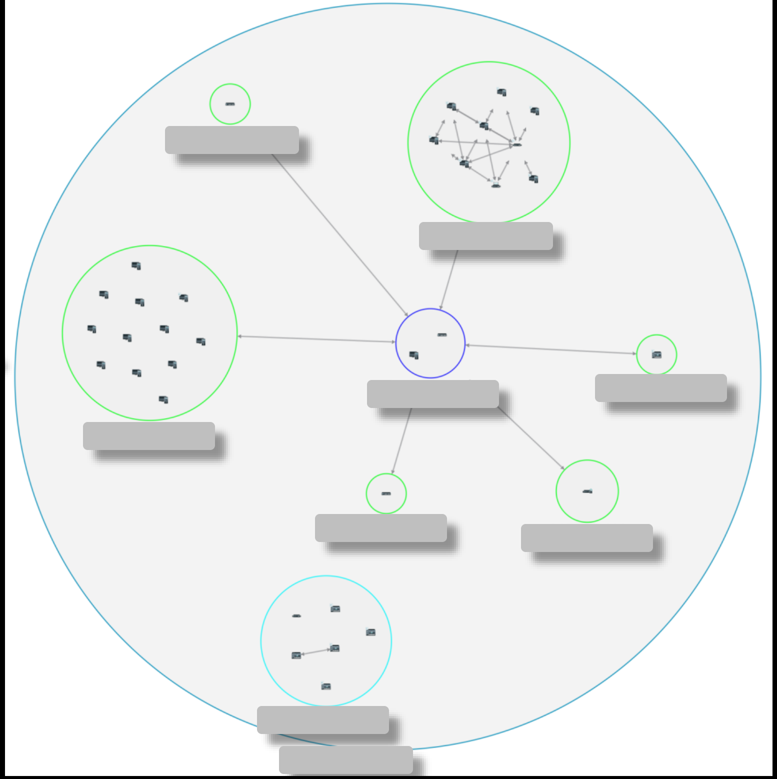
3 OT VISIBILITY & MONITORING

Deploy **Platform** to gain visibility

3 OT VISIBILITY & MONITORING

validating the security controls implemented in a defensible architecture



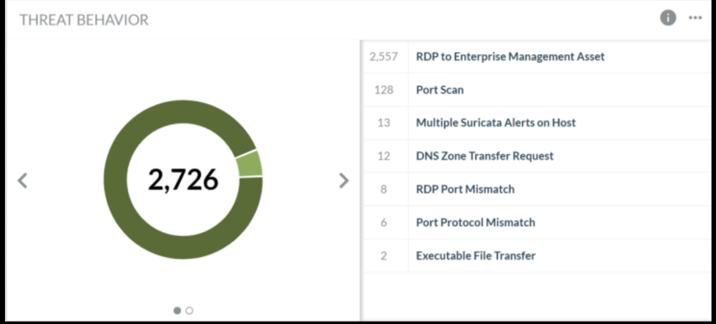


3 OT VISIBILITY & MONITORING

CyberCompare
A BOSCH BUSINESS

Proactive Threat Hunt based on Scenarios

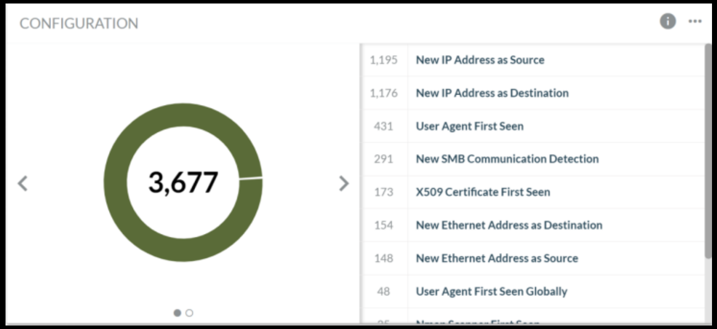
Actively monitor traffic for potential threats



THREAT BEHAVIOR

2,726

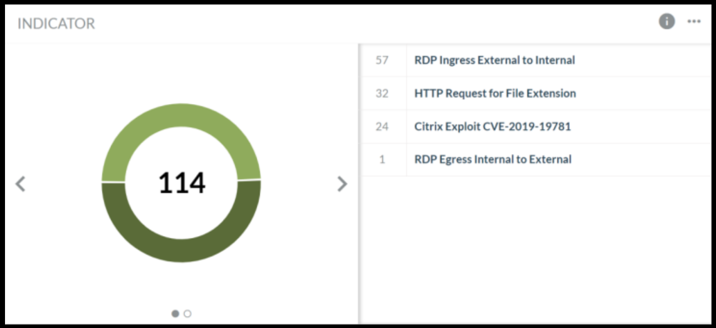
2,557	RDP to Enterprise Management Asset
128	Port Scan
13	Multiple Suricata Alerts on Host
12	DNS Zone Transfer Request
8	RDP Port Mismatch
6	Port Protocol Mismatch
2	Executable File Transfer



CONFIGURATION

3,677

1,195	New IP Address as Source
1,176	New IP Address as Destination
431	User Agent First Seen
291	New SMB Communication Detection
173	X509 Certificate First Seen
154	New Ethernet Address as Destination
148	New Ethernet Address as Source
48	User Agent First Seen Globally
[illegible]	Nmap Scanner First Seen



INDICATOR

114

57	RDP Ingress External to Internal
32	HTTP Request for File Extension
24	Citrix Exploit CVE-2019-19781
1	RDP Egress Internal to External

2 DEFENSIBLE ARCHITECTURE

After the initial Network/Risk Assesment and Platform Deployment

Safety system segmentation

Mitigating high risk unencrypted ot communication links

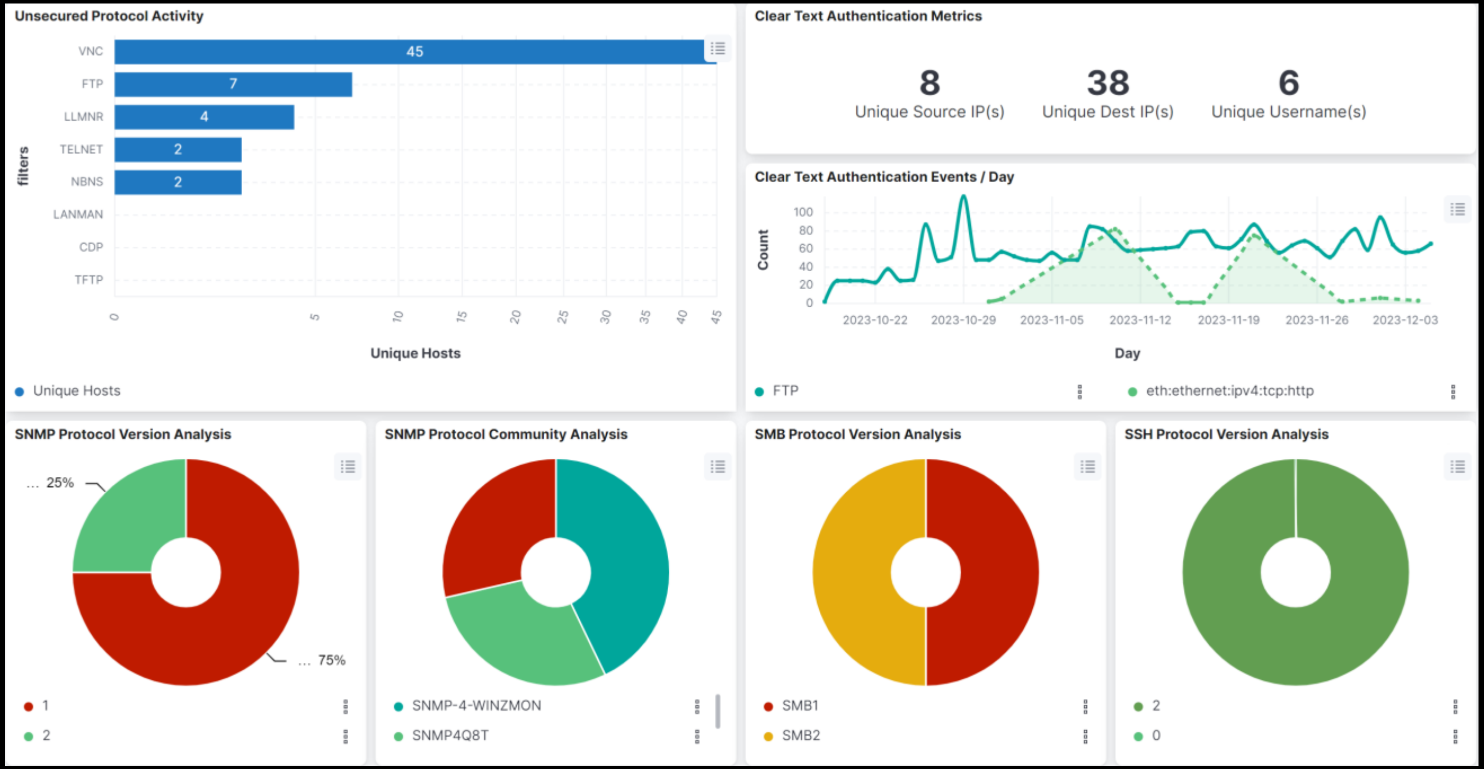
Establishing isolation procedures

OT security use cases and specific training for SOC

2 DEFENSIBLE ARCHITECTURE

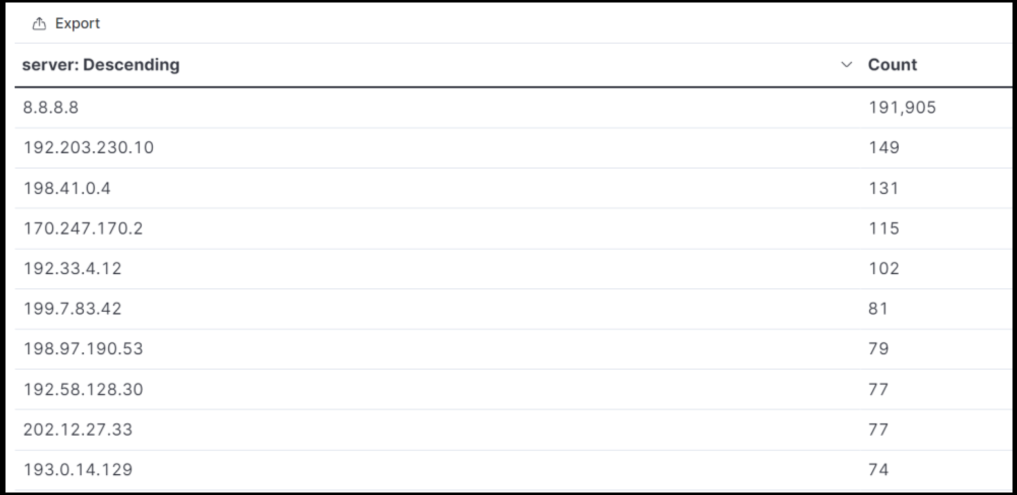
Dragos identified eight vulnerable/unsecure protocols

- HTTP
- FTP
- SMB v1
- DHCPv6
- SNMP v1 v2
- Unencrypted LDAP
- NBNS
- LLMNR



2 DEFENSIBLE ARCHITECTURE

Dragos identified that devices in the OT networks can contact external servers by sending Domain Name Service (DNS) protocol requests to external addresses directly from L3 domain controllers or indirectly via recursive lookups



Export

server: Descending	Count
8.8.8.8	191,905
192.203.230.10	149
198.41.0.4	131
170.247.170.2	115
192.33.4.12	102
199.7.83.42	81
198.97.190.53	79
192.58.128.30	77
202.12.27.33	77
193.0.14.129	74

The Dragos platform shows multiple outbound DNS requests and corresponding responses.

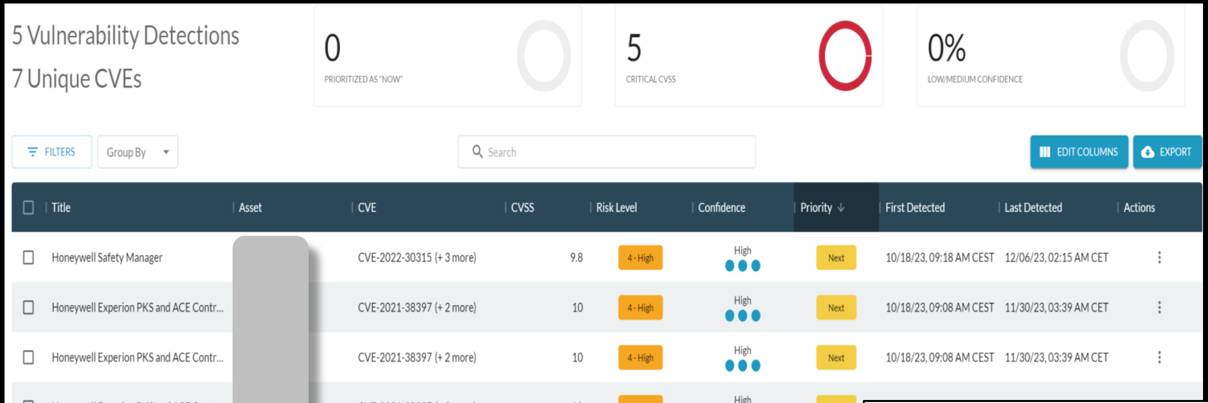
Over 70% of external DNS traffic occurs from the domain controller

5

RISK-BASED VULNERABILITY MANAGEMENT

CyberCompare
A BOSCH BUSINESS

Knowing your vulnerabilities: Location based analysis



5 Vulnerability Detections
7 Unique CVEs

0 PRIORITIZED AS "NOW"

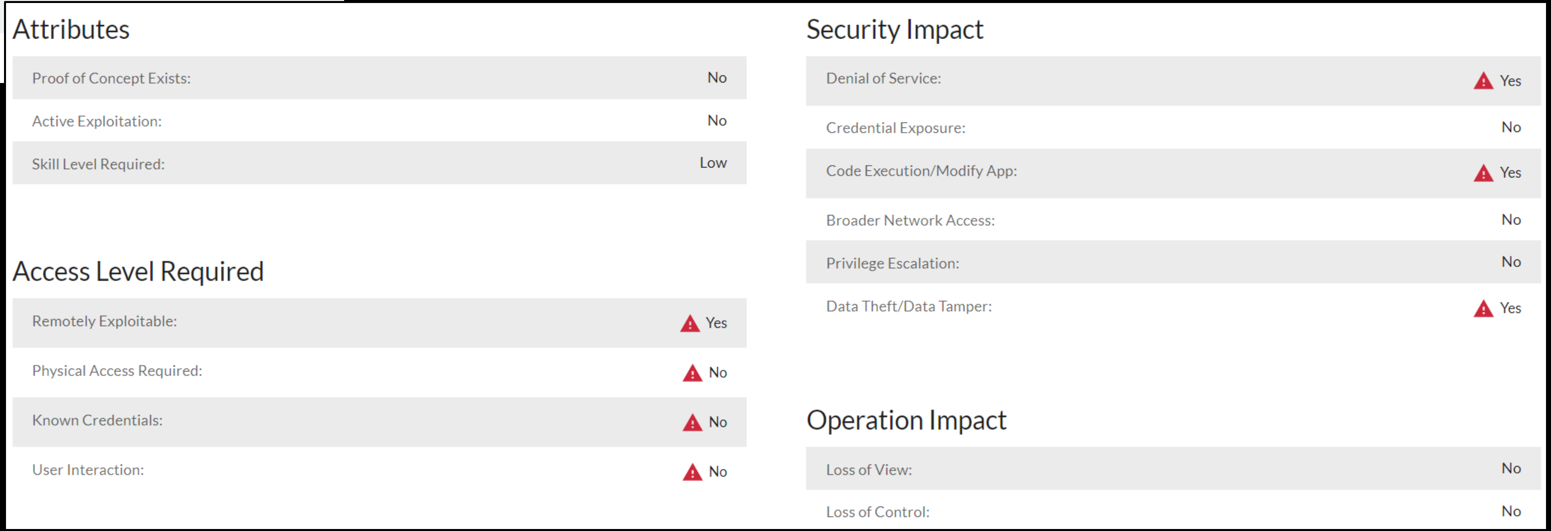
5 CRITICAL CVSS

0% LOW/MEDIUM CONFIDENCE

□	Title	Asset	CVE	CVSS	Risk Level	Confidence	Priority ↓	First Detected	Last Detected	Actions
□	Honeywell Safety Manager	[redacted]	CVE-2022-30315 (+ 3 more)	9.8	4 - High	High ●●●	Next	10/18/23, 09:18 AM CEST	12/06/23, 02:15 AM CET	⋮
□	Honeywell Experion PKS and ACE Contr...	[redacted]	CVE-2021-38397 (+ 2 more)	10	4 - High	High ●●●	Next	10/18/23, 09:08 AM CEST	11/30/23, 03:39 AM CET	⋮
□	Honeywell Experion PKS and ACE Contr...	[redacted]	CVE-2021-38397 (+ 2 more)	10	4 - High	High ●●●	Next	10/18/23, 09:08 AM CEST	11/30/23, 03:39 AM CET	⋮
□	Honeywell Experion PKS and ACE Contr...	[redacted]	CVE-2021-38397 (+ 2 more)	10	4 - High	High ●●●	Next			
□	Honeywell Experion PKS and ACE Contr...	[redacted]	CVE-2021-38397 (+ 2 more)	10	4 - High	High ●●●	Next			

Key Switch Position allowing Forced Values

-> Prevent remote "force enable"



Attributes

Proof of Concept Exists:	No
Active Exploitation:	No
Skill Level Required:	Low

Access Level Required

Remotely Exploitable:	⚠ Yes
Physical Access Required:	⚠ No
Known Credentials:	⚠ No
User Interaction:	⚠ No

Security Impact

Denial of Service:	⚠ Yes
Credential Exposure:	No
Code Execution/Modify App:	⚠ Yes
Broader Network Access:	No
Privilege Escalation:	No
Data Theft/Data Tamper:	⚠ Yes

Operation Impact

Loss of View:	No
Loss of Control:	No

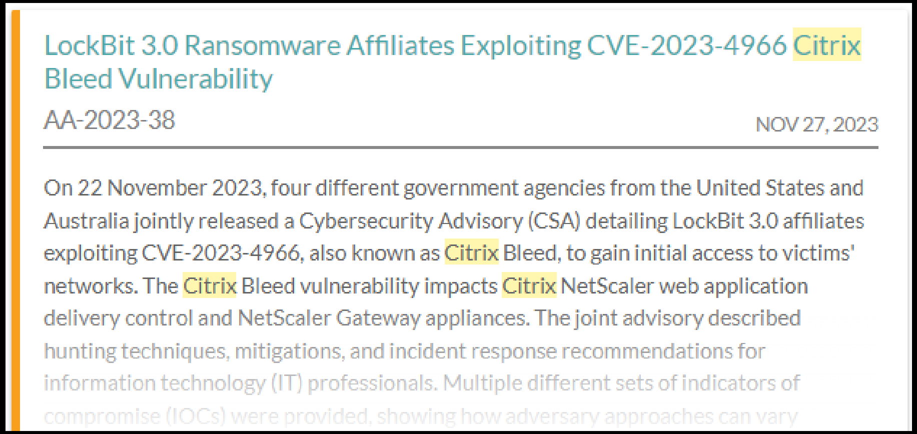
4 SECURE REMOTE ACCESS / MFA

CyberCompare
A BOSCH BUSINESS

Citrix remote access solution in place

MFA enabled

But (5): *"Know your vulnerabilities"*

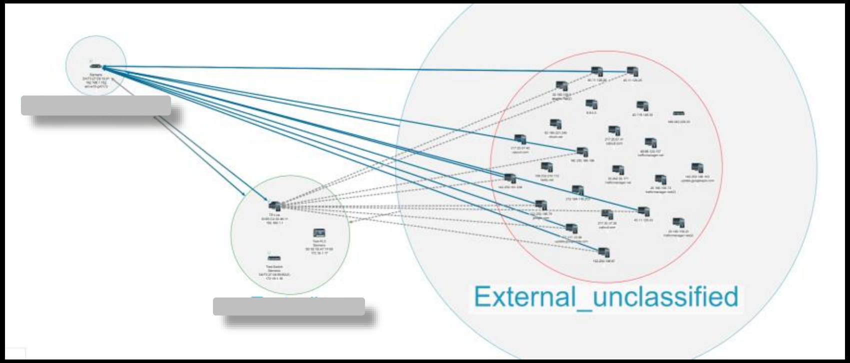


LockBit 3.0 Ransomware Affiliates Exploiting CVE-2023-4966 Citrix Bleed Vulnerability

AA-2023-38 NOV 27, 2023

On 22 November 2023, four different government agencies from the United States and Australia jointly released a Cybersecurity Advisory (CSA) detailing LockBit 3.0 affiliates exploiting CVE-2023-4966, also known as Citrix Bleed, to gain initial access to victims' networks. The Citrix Bleed vulnerability impacts Citrix NetScaler web application delivery control and NetScaler Gateway appliances. The joint advisory described hunting techniques, mitigations, and incident response recommendations for information technology (IT) professionals. Multiple different sets of indicators of compromise (IOCs) were provided, showing how adversary approaches can vary

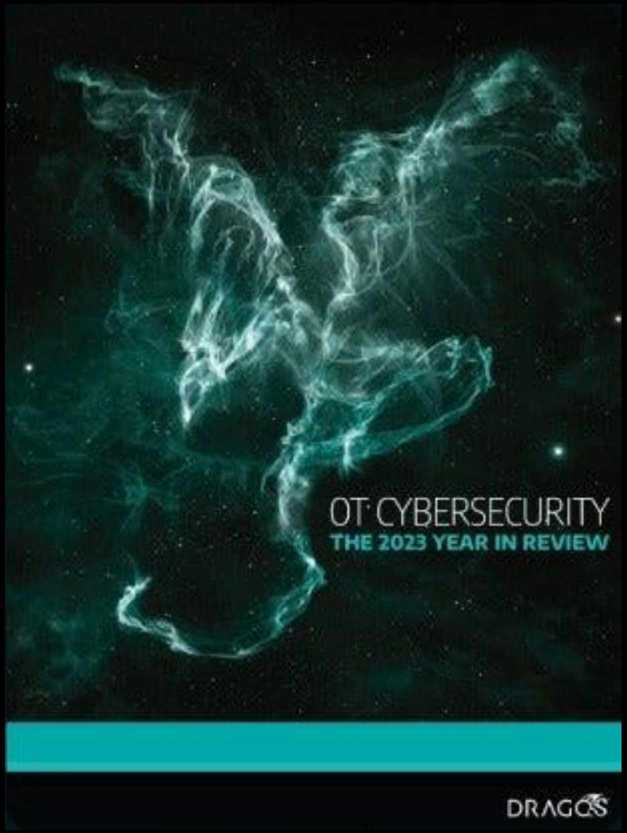
And (3): *"Use Visibility"*



THANK YOU

Oliver Herterich
Senior Solution Architect DACH & EE

oherterich@dragos.com
O: +49 175 419 1079



Ressources:

Dragos Year in Review 2023:
https://www.dragos.com/ot-cybersecurity-year-in-review/#anchor-report

SANS Whitepaper – 5 Critical Controls:
https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

FACE THE UNPREDICTABLE

Ganzheitliche IT-/OT-Security

XDR-Plattform von TEHTRIS

TEHTRIS

FACE THE UNPREDICTABLE

Agenda

Ausgangslage 01

02 Managed XDR

Mehrwerte 03

/01

Ausgangslage

Ausgangslage

Betreiber einer kritischen Infrastruktur (Energie)

Kleine bis mittlere IT-Abteilung (wenig Ressourcen)

ISO 27001 zertifiziert

KRITIS => BSI SZA (System zur Angriffserkennung)

Ausgangslage

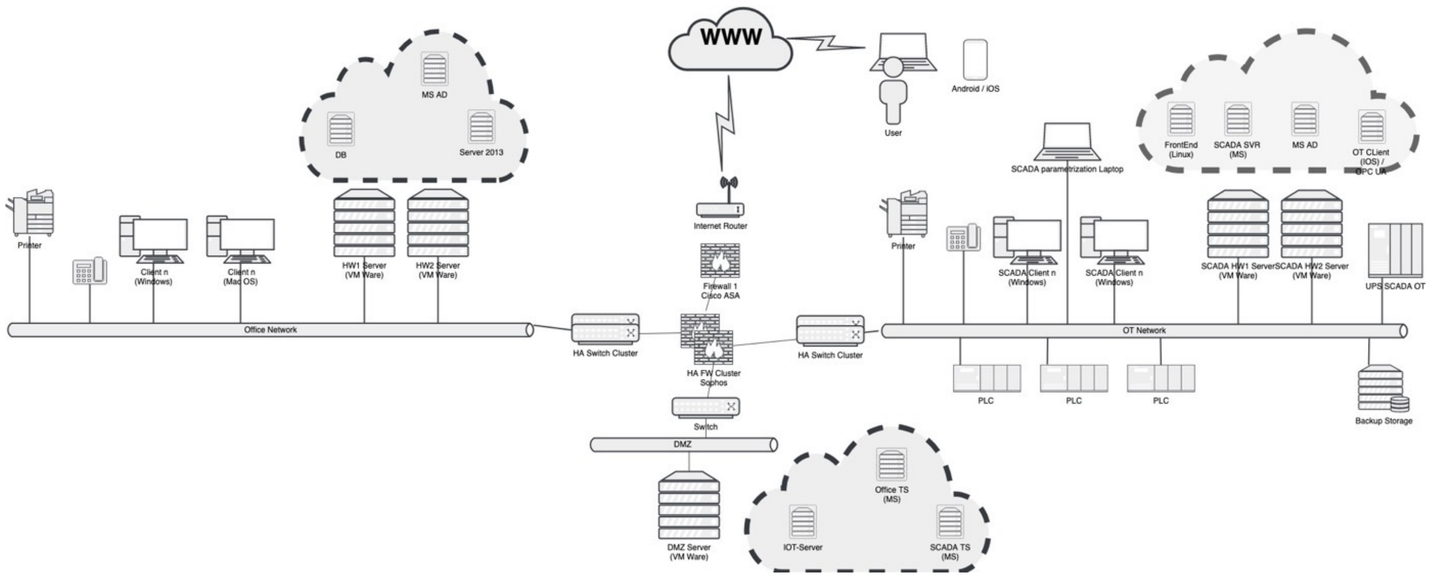
Betreiber einer kritischen Infrastruktur (Energie)

Bestand:

- Endpoint-Security Lösung implementiert (bedingt gepflegt)
- Anomaly-Detection-Lösung auf Basis von NIDS (in der Teststellung)

Offen:

- SIEM (Log-Überwachung)

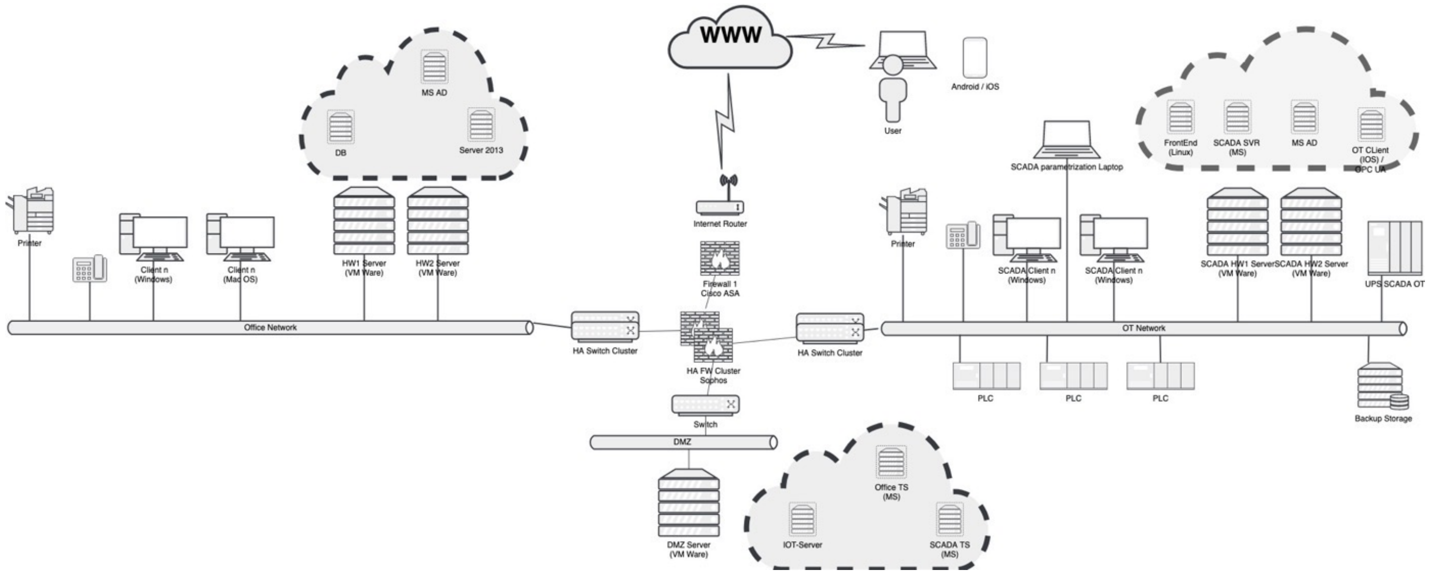


Ausgangslage

Betreiber einer kritischen Infrastruktur (Energie)

Herausforderungen des Kunden:

- Pflege und Bedienung von min. 3 Security Tools
- Bei gleicher Personalstärke

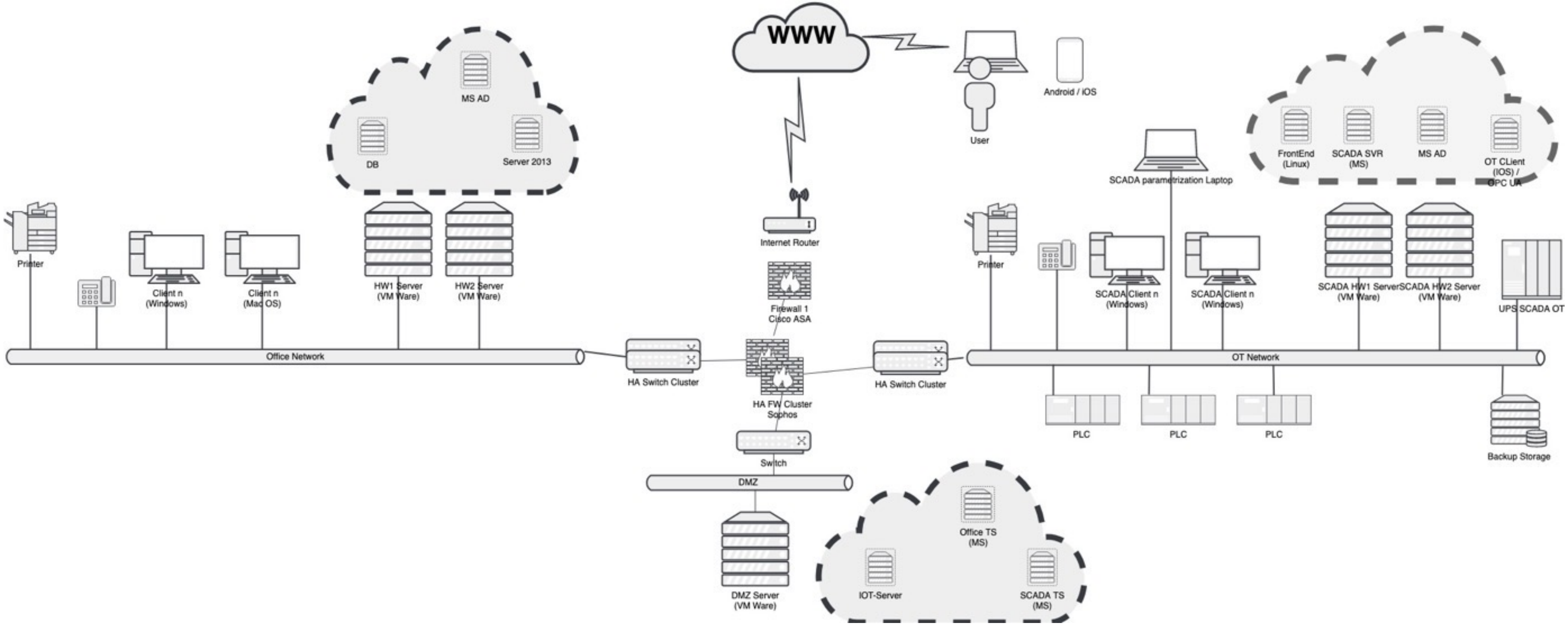


/02

Managed XDR

Zentrale holistische Lösung zur IT-/OT-Security

IT/OT Infrastruktur

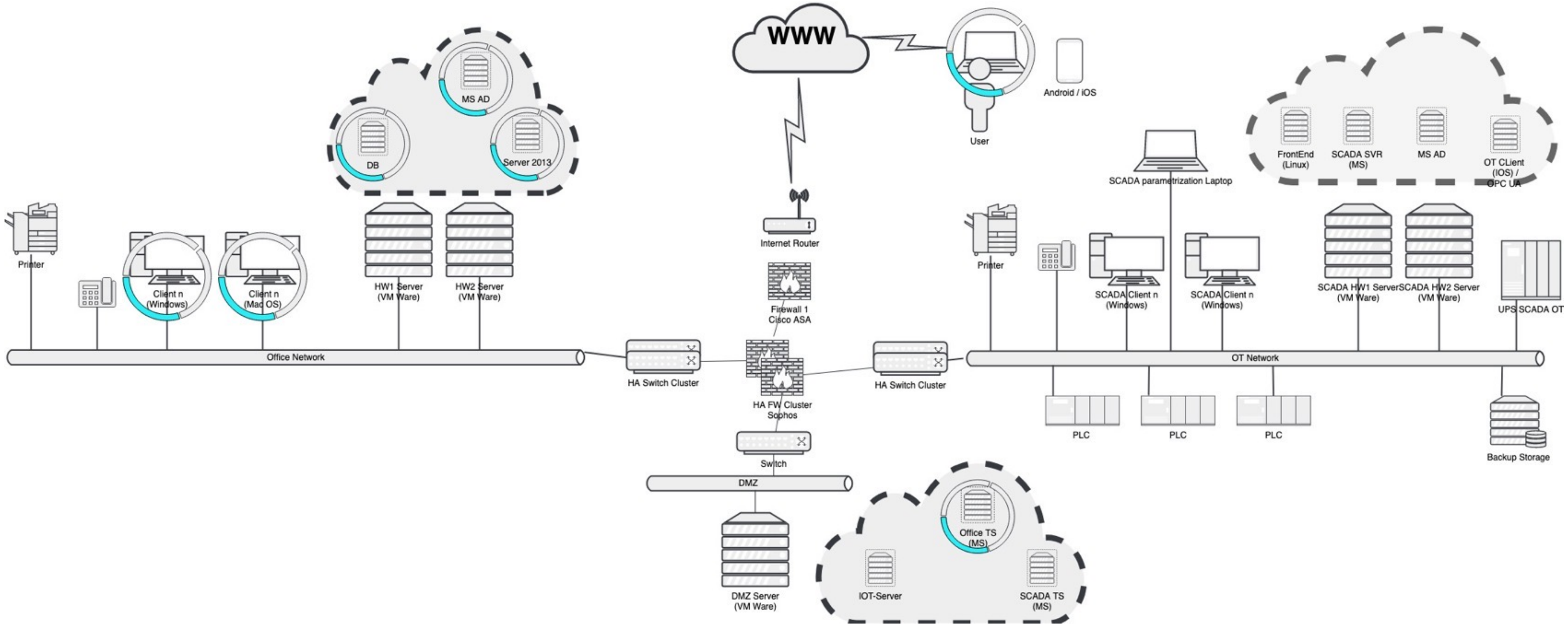


Zentrale holistische Lösung zur IT-/OT-Security

EPP (Endpoint Protection Platform / AV)

EPP

Datei



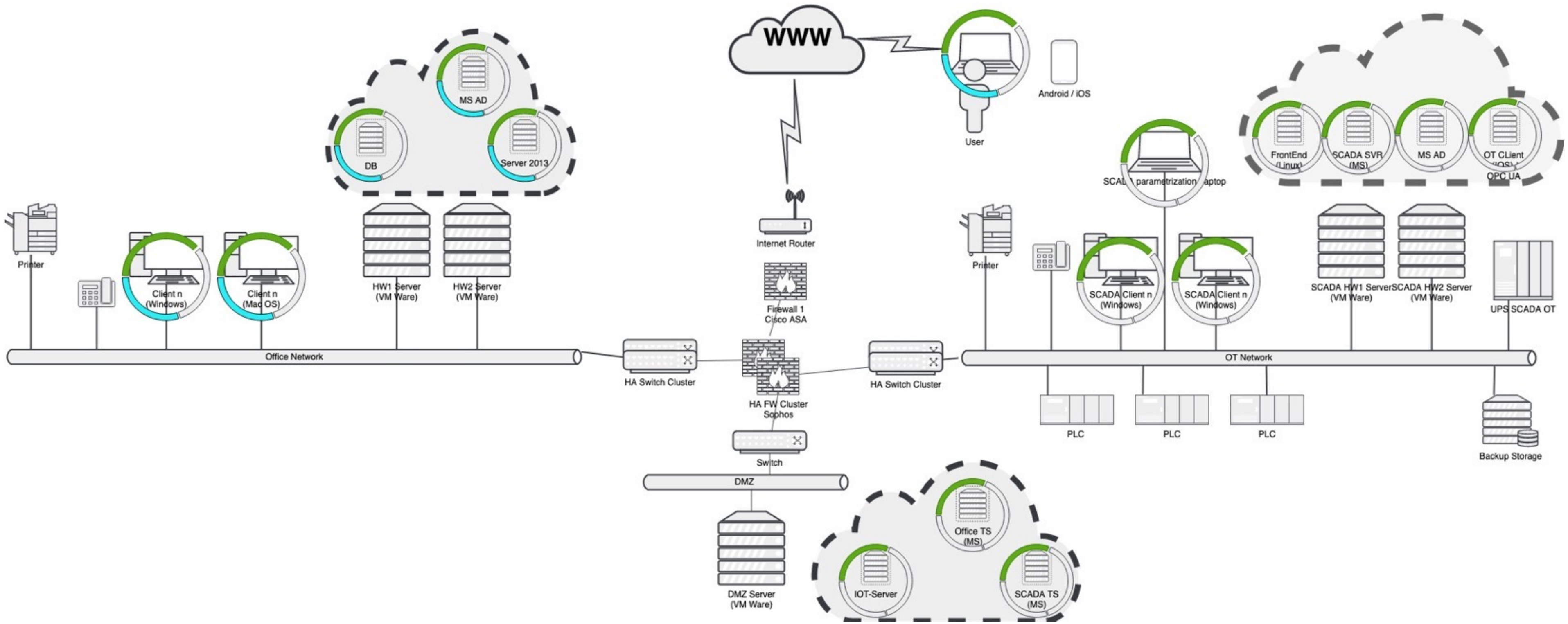
Zentrale holistische Lösung zur IT-/OT-Security

EDR (Endpoint Detection Responce)

EDR

Dateien

Anwendungen / Prozesse

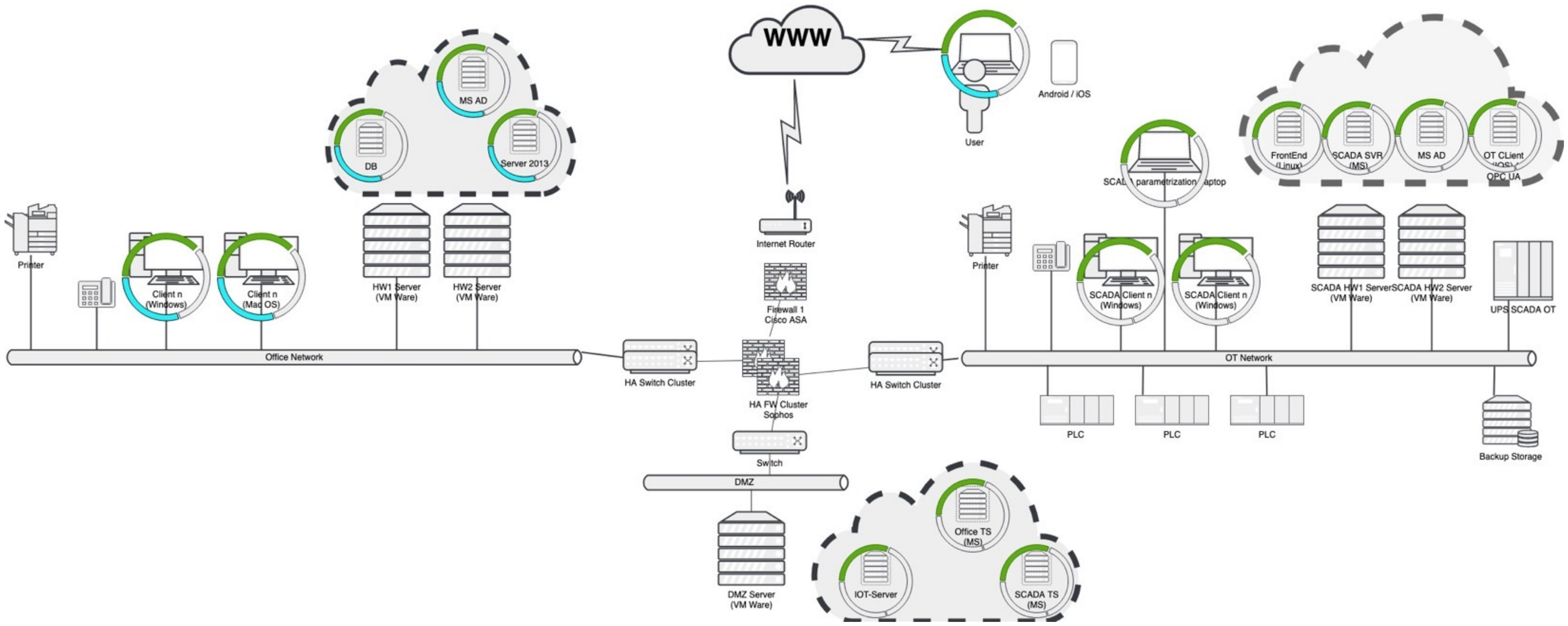


Zentrale holistische Lösung zur IT-/OT-Security

Dateien

Anwendungen / Prozesse

Logdateien



Zentrale holistische Lösung zur IT-/OT-Security

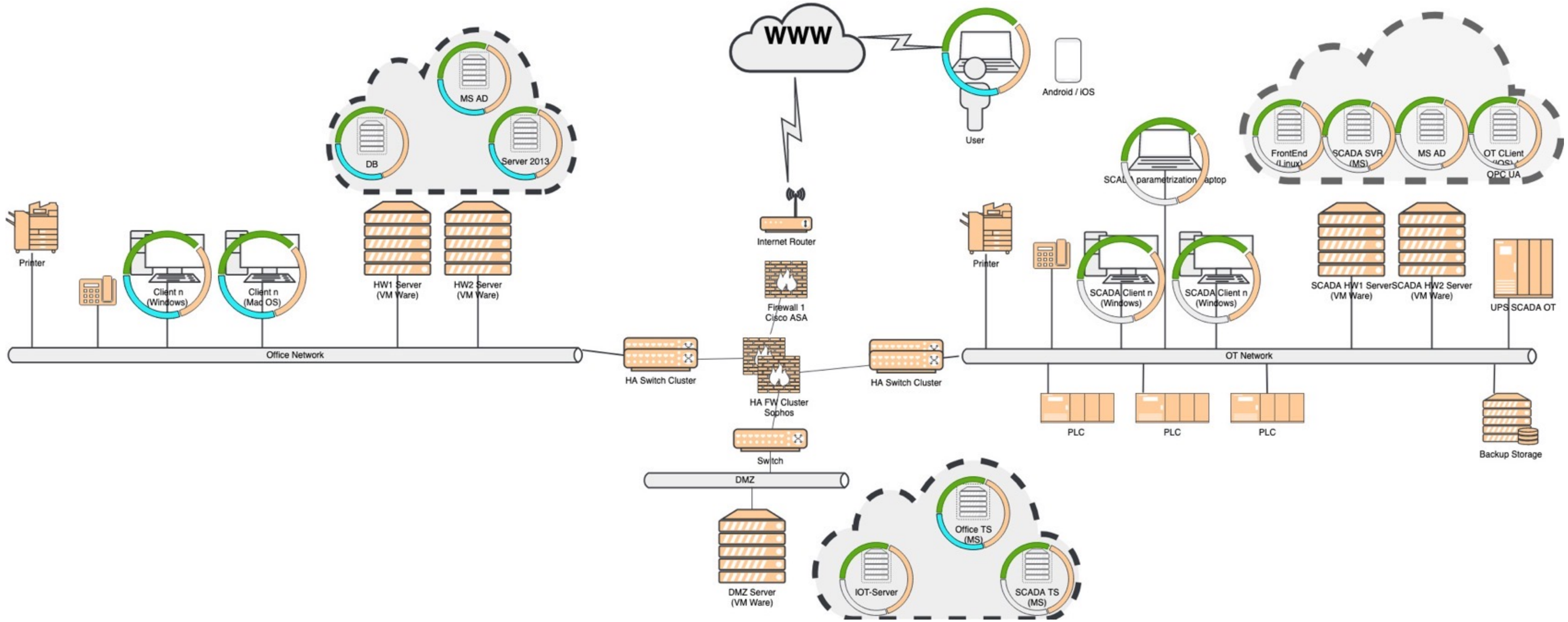
SIEM (Security Information Event Management)

SIEM

Dateien

Anwendungen / Prozesse

Logdateien

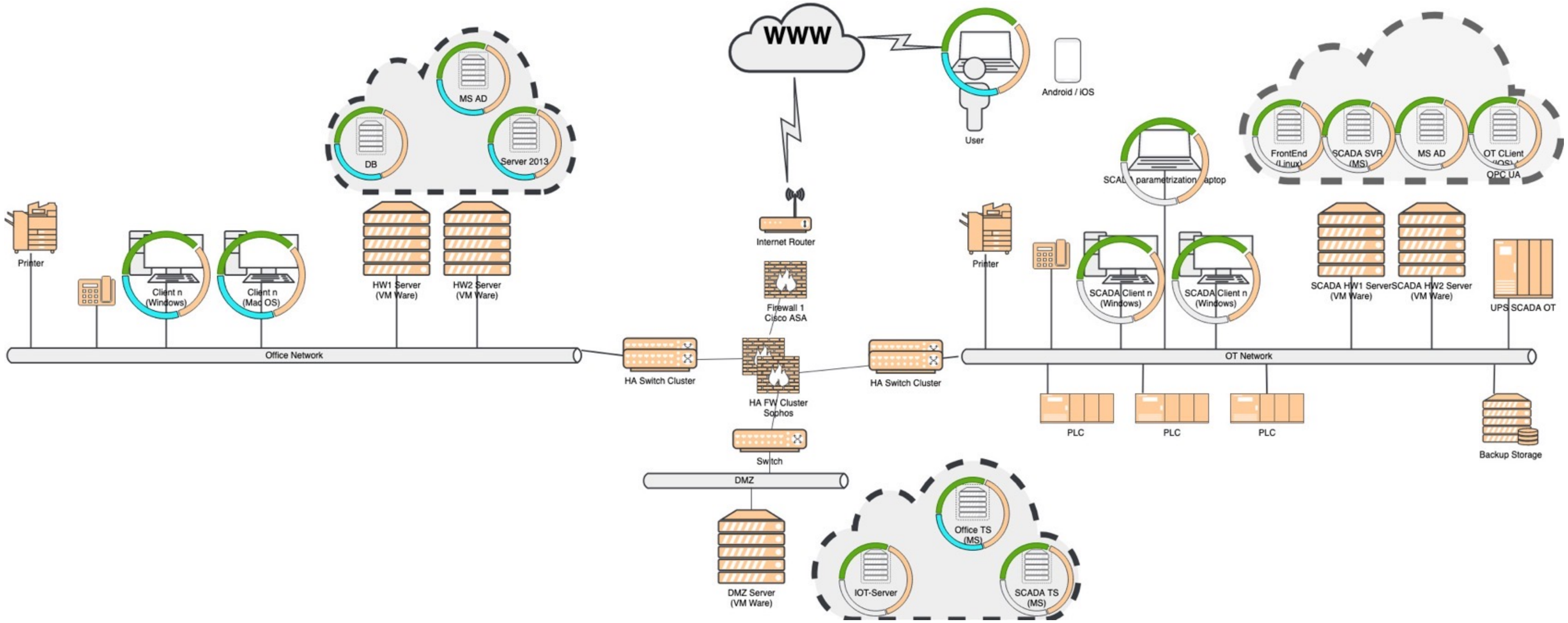


Zentrale holistische Lösung zur IT-/OT-Security

Dateien

Anwendungen / Prozesse

Logdateien



Zentrale holistische Lösung zur IT-/OT-Security

NTA (Network Traffic Analysis)

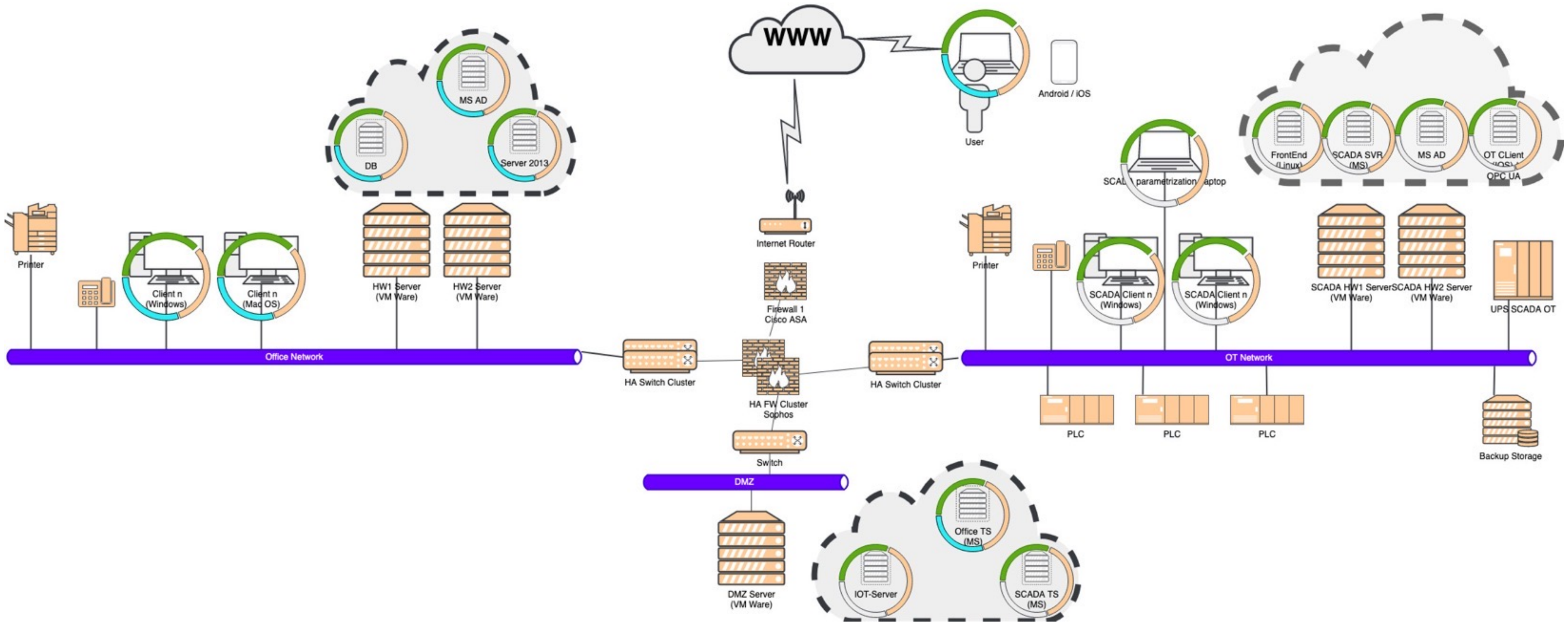
NTA

Dateien

Anwendungen / Prozesse

Logdateien

Netzwerk



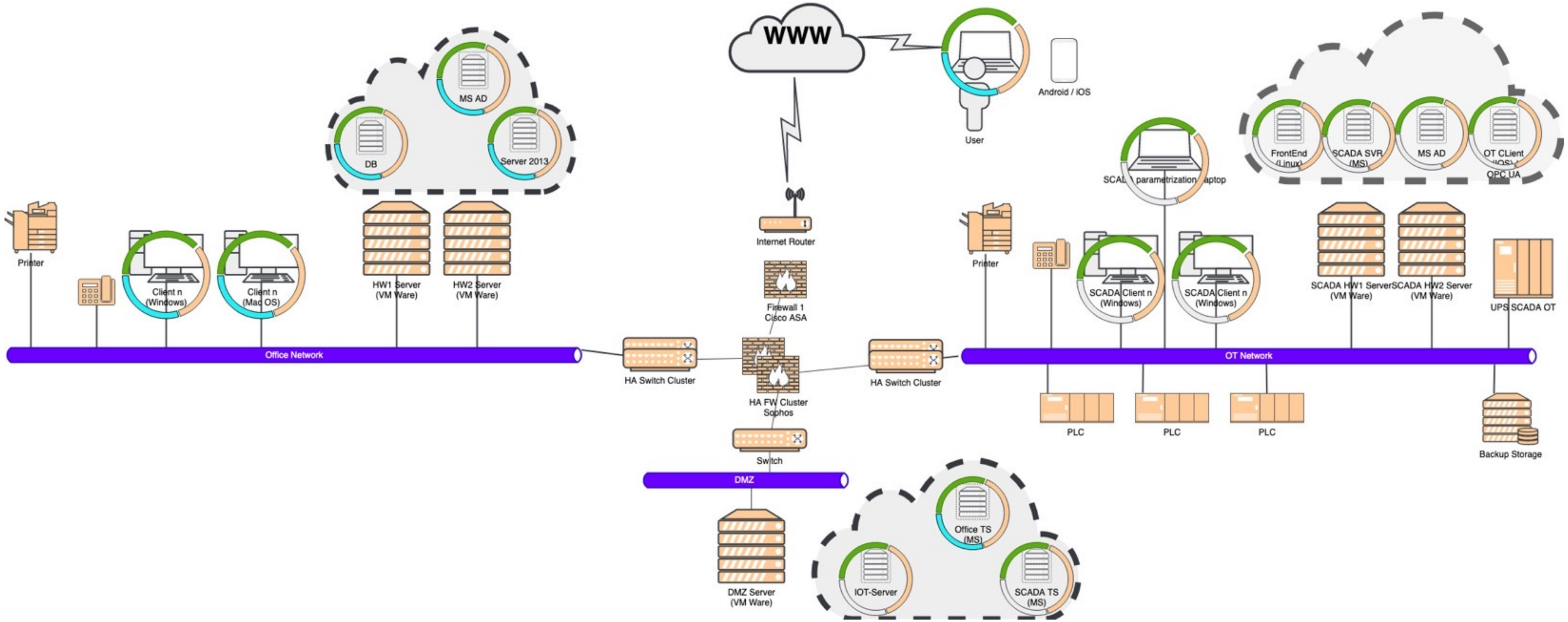
Zentrale holistische Lösung zur IT-/OT-Security

Dateien

Anwendungen / Prozesse

Logdateien

Netzwerk



Zentrale holistische Lösung zur IT-/OT-Security

MTD (Mobile Threat Detection)

MTD

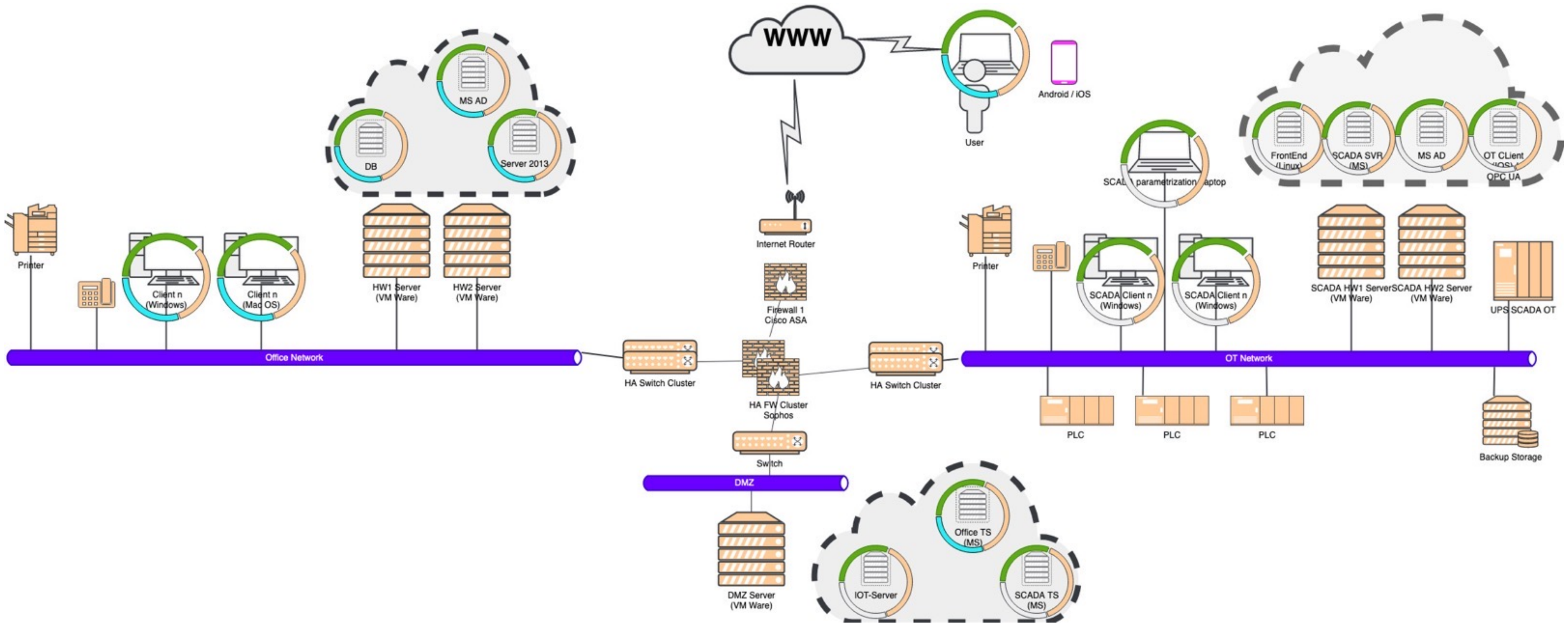
Dateien

Anwendungen / Prozesse

Logdateien

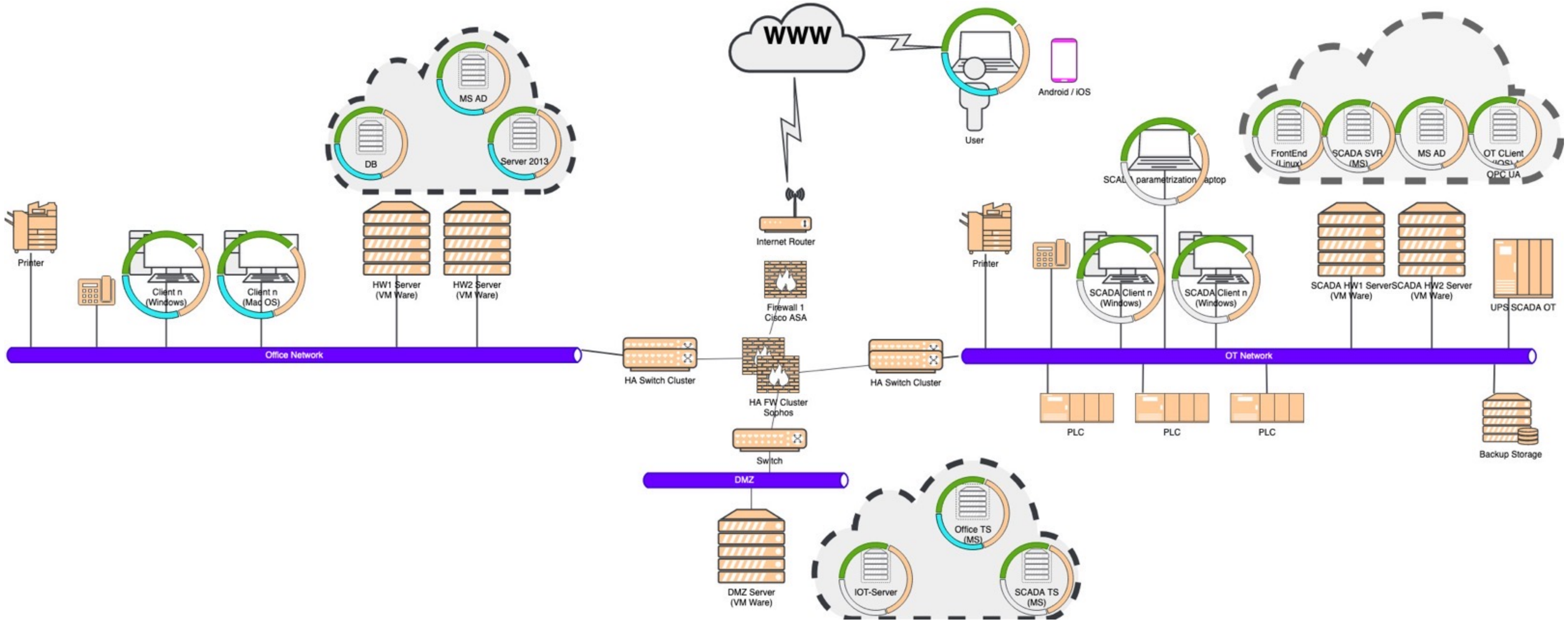
Network

Mobile



Zentrale holistische Lösung zur IT-/OT-Security

- Dateien
- Anwendungen / Prozesse
- Logdateien
- Network
- Mobile

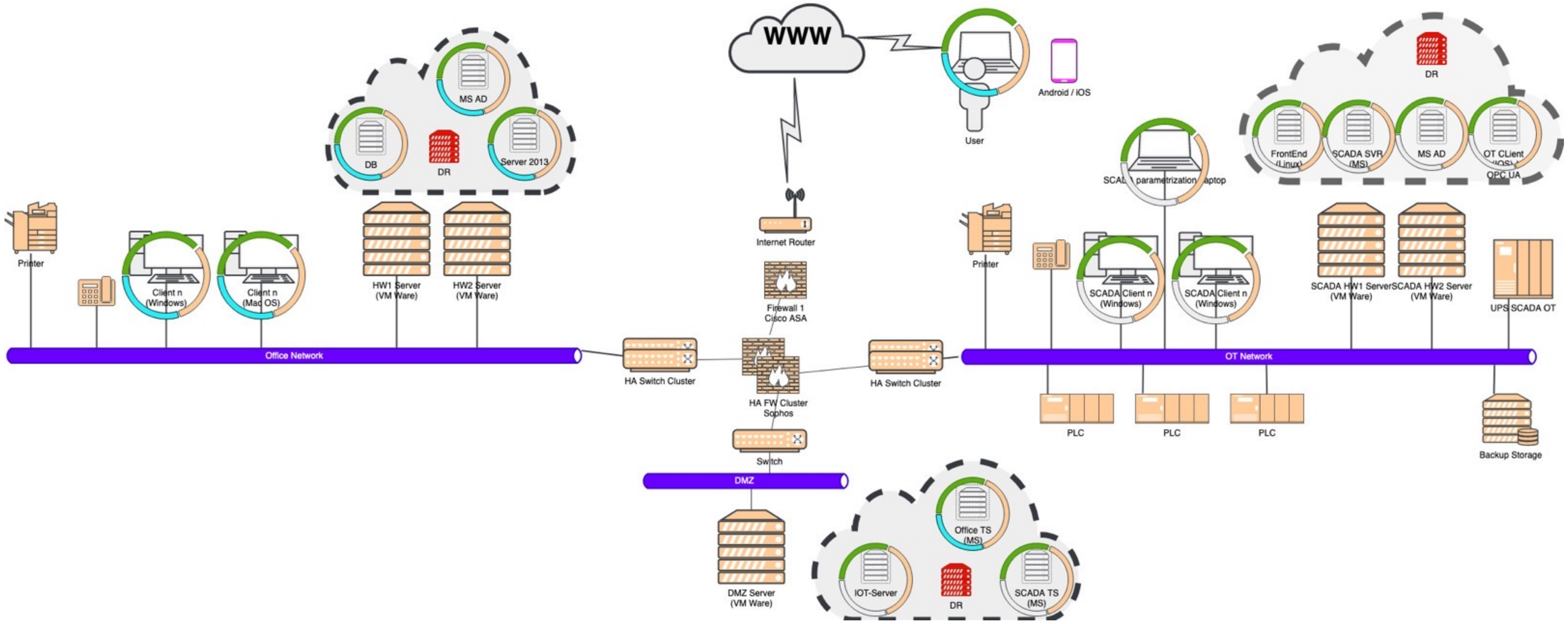


Zentrale holistische Lösung zur IT-/OT-Security

DR (Deceptive Response)

Deceptive Response

- Dateien
- Anwendungen / Prozesse
- Logdateien
- Network
- Mobile
- Honeypot



Zentrale holistische Lösung zur IT-/OT-Security

XDR (eXtended Detection and Response)

SOC

OVH Frankfurt / **CLIENT DEDICATED SERVERS**

TEHTRIS XDR Platform

Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence
Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

CYBER DATA LAKE

EPP

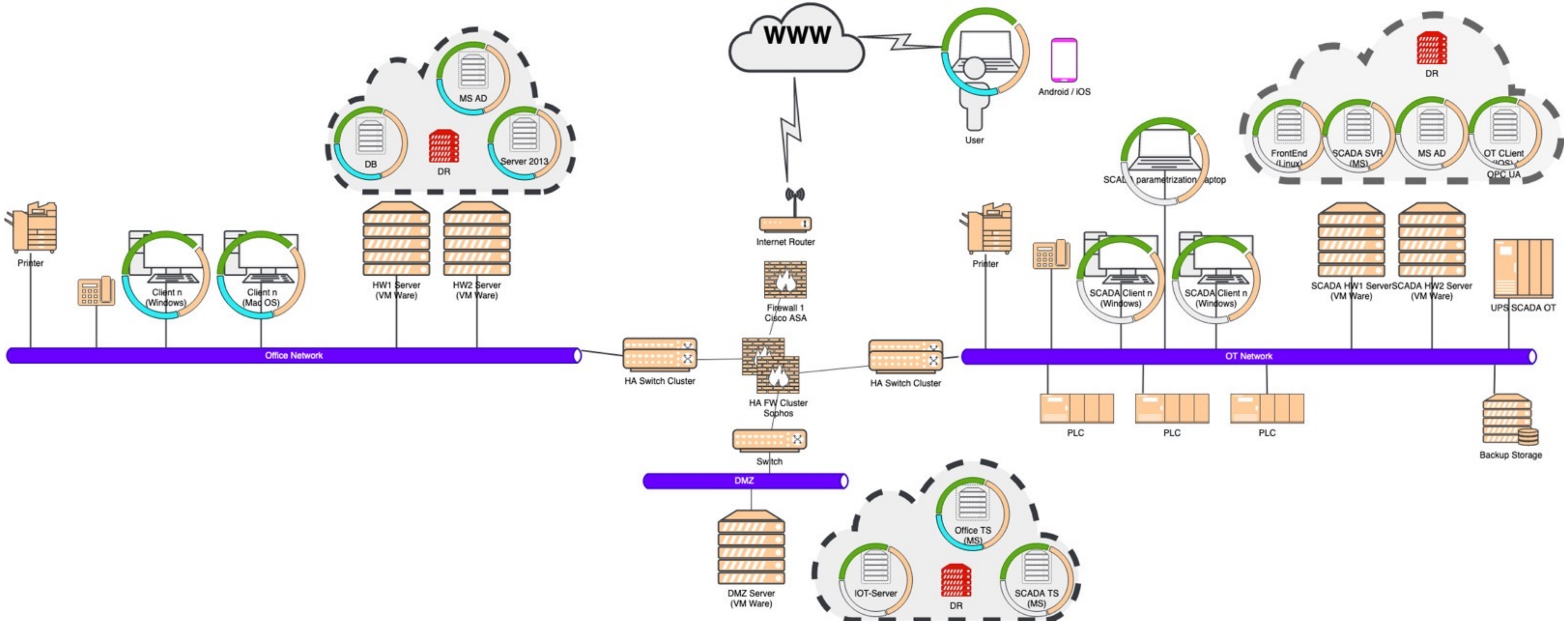
NTA

EDR

MTD

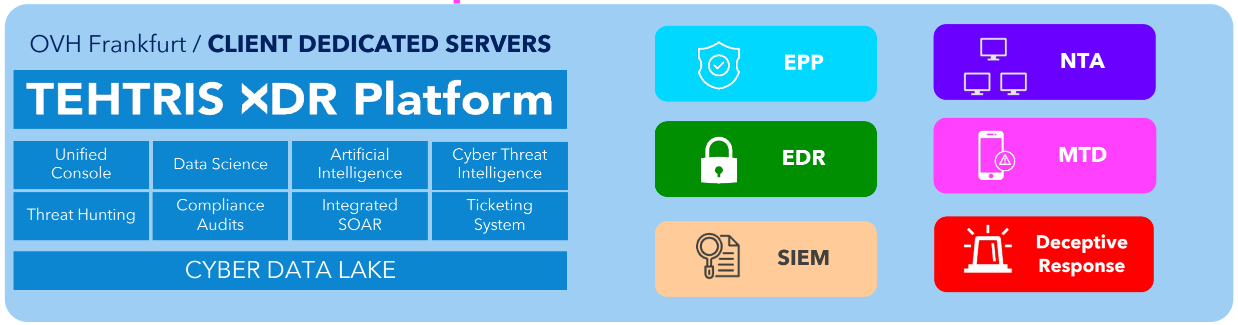
SIEM

Deceptive Response



Zentrale holistische Lösung zur IT-/OT-Security

XDR (eXtended Detection and Response)



OVH Frankfurt / **CLIENT DEDICATED SERVERS**

TEHTRIS XDR Platform

Unified Console	Data Science	Artificial Intelligence	Cyber Threat Intelligence
Threat Hunting	Compliance Audits	Integrated SOAR	Ticketing System

CYBER DATA LAKE

EPP

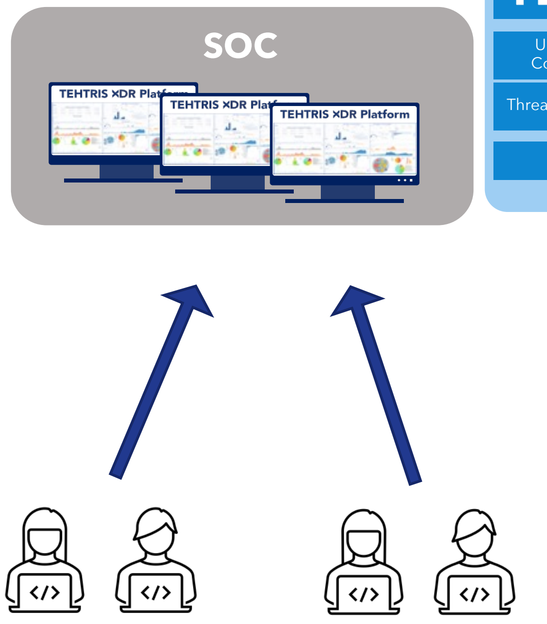
EDR

SIEM

NTA

MTD

Deceptive Response

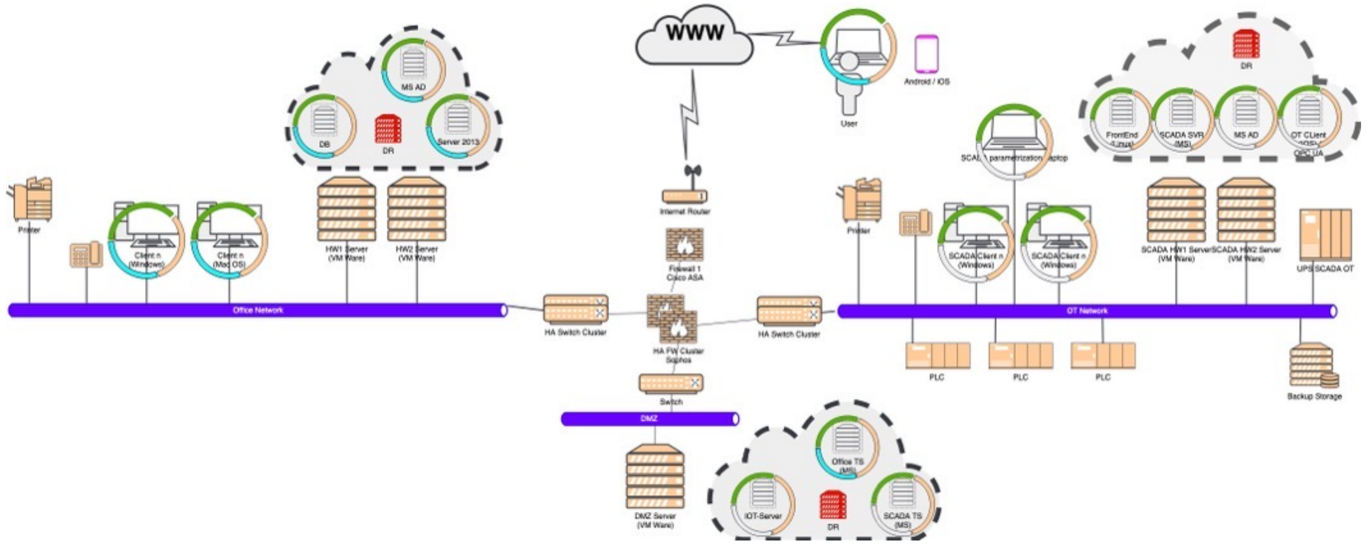


SOC

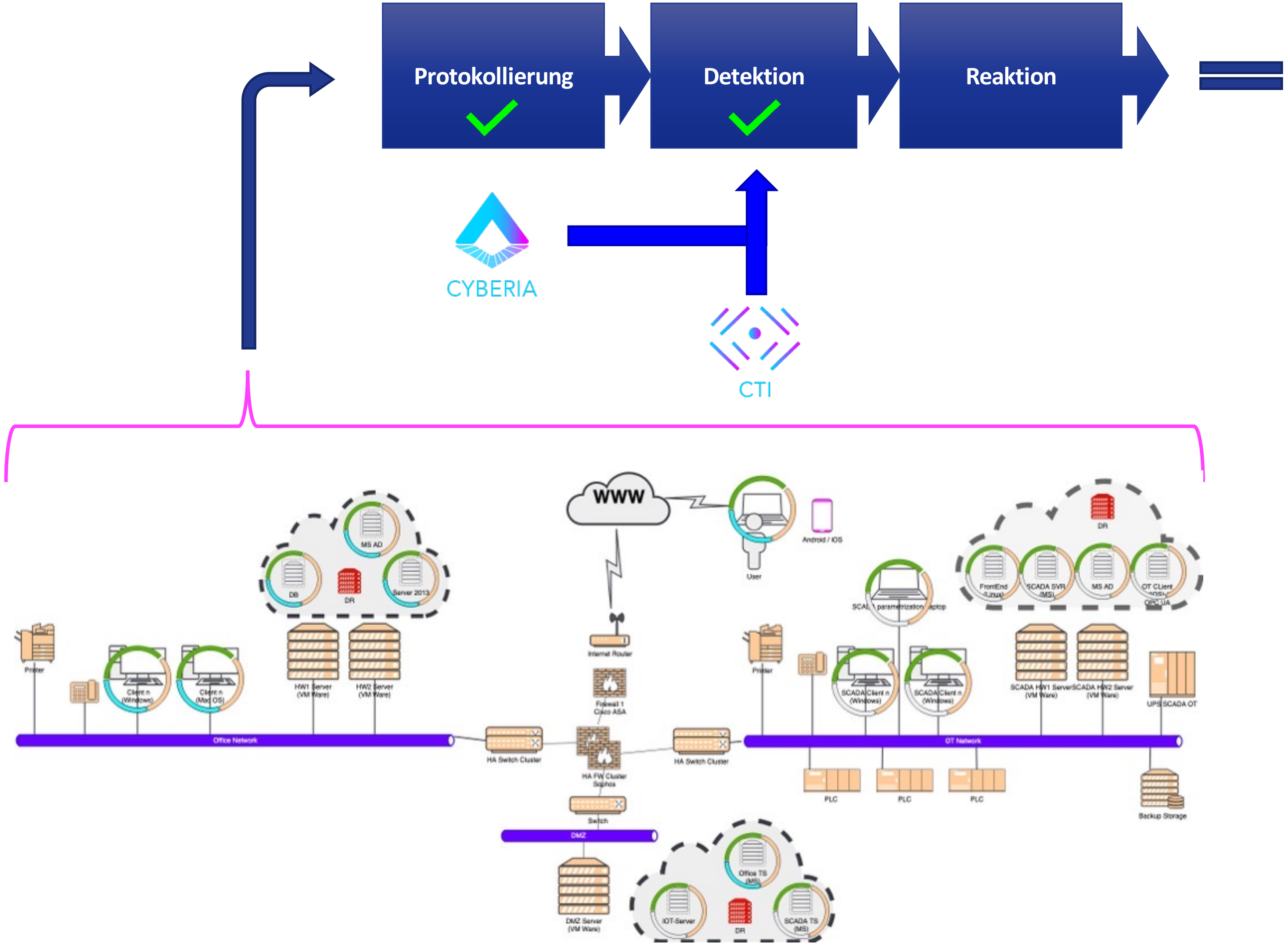
SOC-Team

(Partner / TEHTRIS)

Kunden IT



Zentrale holistische Lösung zur IT-/OT-Security



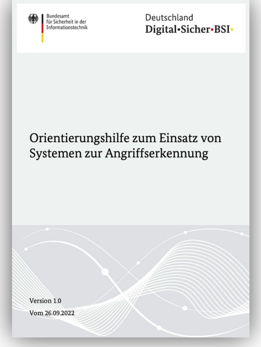
Protokollierung ✓

Detektion ✓

Reaktion

CYBERIA

CTI



Bundesamt
für Sicherheit in der
Informationstechnik

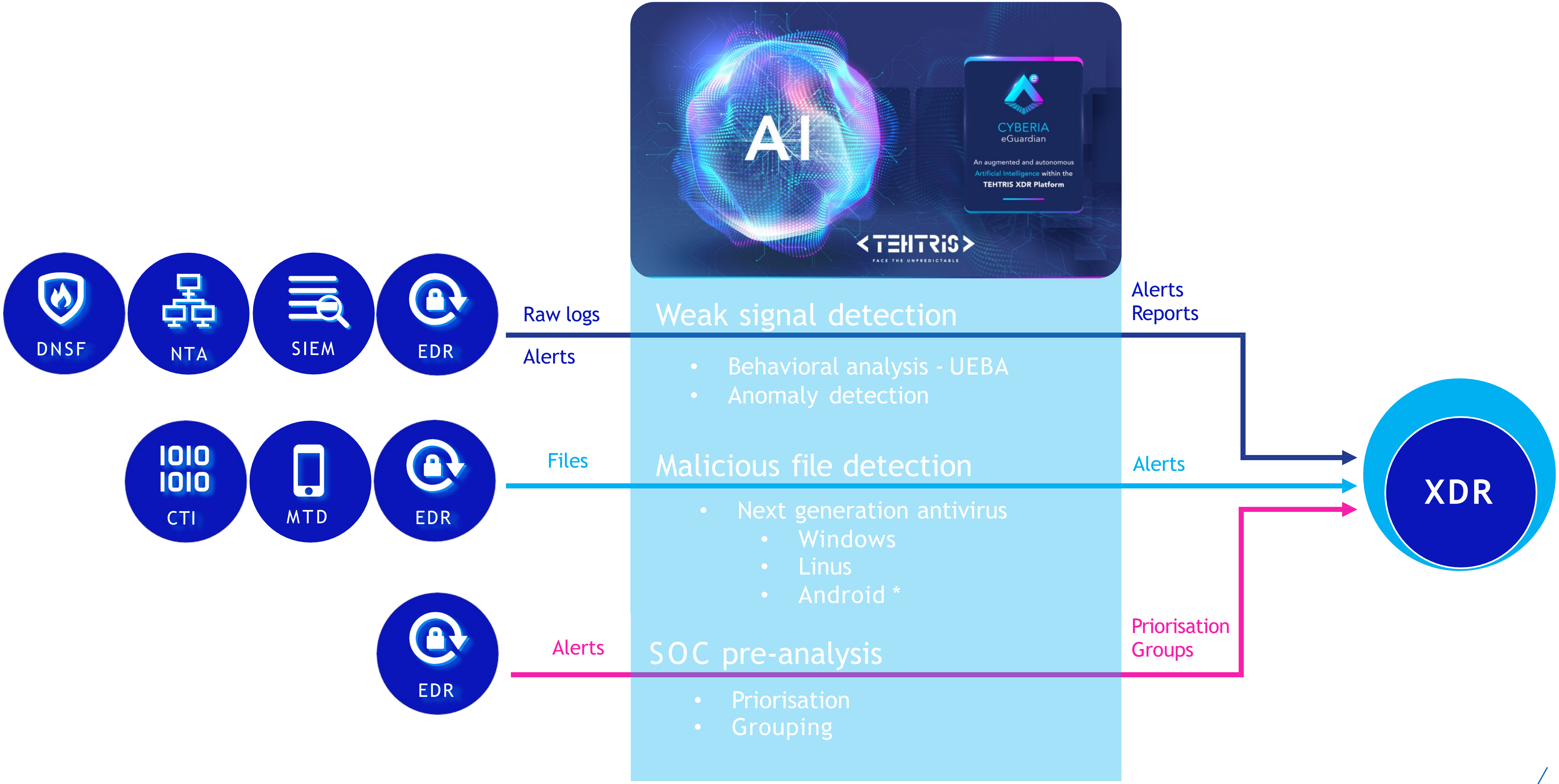
Deutschland
Digital•Sicher•BSI•

Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

Version 1.0

Vom 26.09.2022

Was sind die wichtigsten Funktionen von Cyberia?



Weak signal detection

- Behavioral analysis - UEBA
- Anomaly detection

Malicious file detection

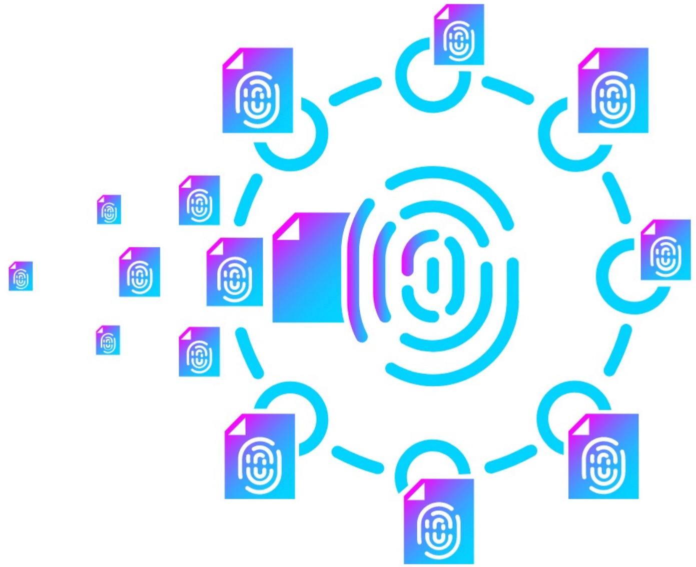
- Next generation antivirus
  - Windows
  - Linus
  - Android *

SOC pre-analysis

- Priorisation
- Grouping

Was ist eine Cyber Threat Intelligence-Plattform?

Wissensdatenbank



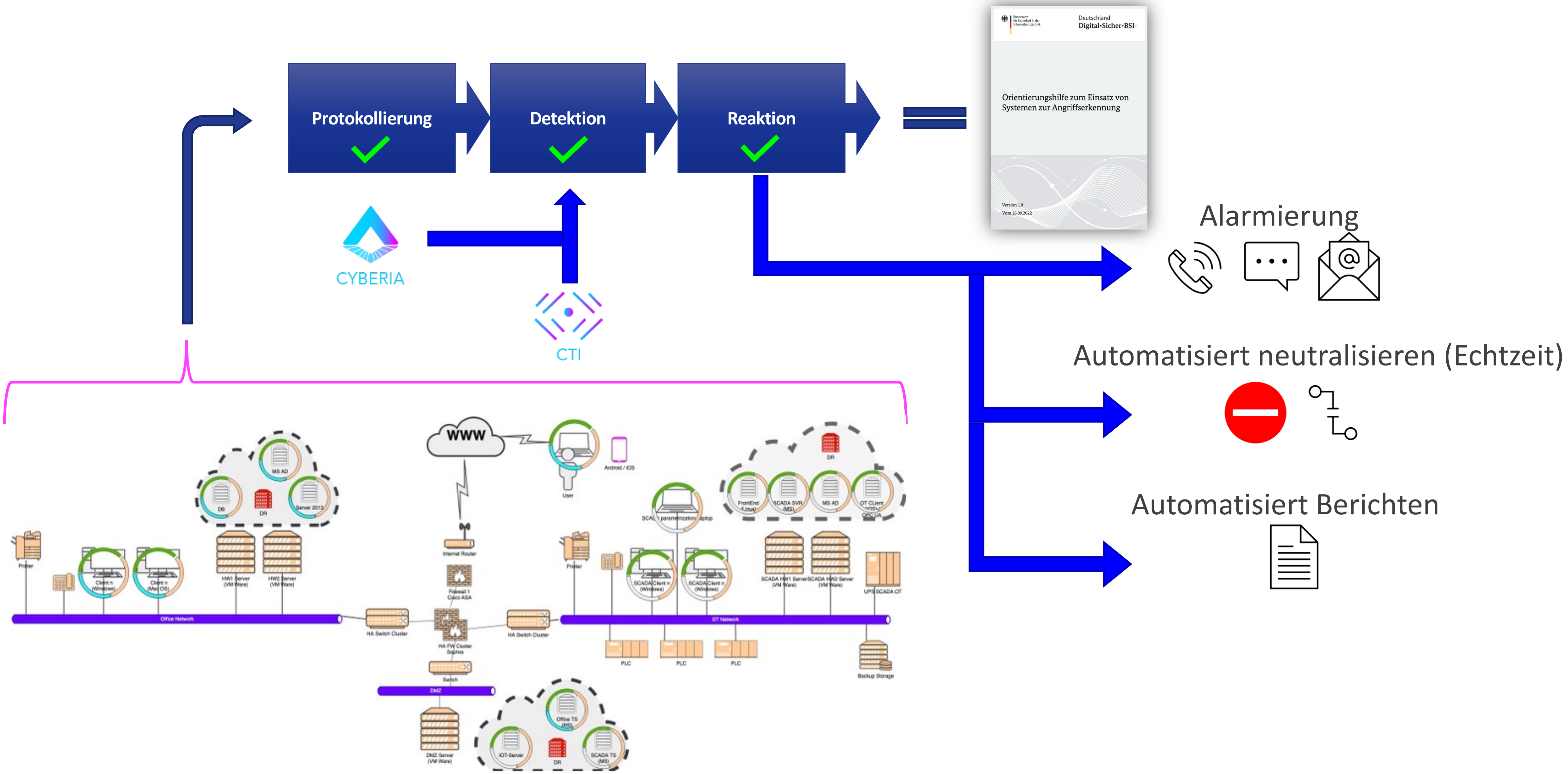
TEHTRIS Quellen:

CYBER THREAT ALLIANCE

...

https://www.youtube.com/watch?v=4UOeo4Z476s

Zentrale holistische Lösung zur IT-/OT-Security



Protokollierung ✓

Detektion ✓

Reaktion ✓

=

Bundesamt für Sicherheit in der Informationstechnik

Deutschland
Digital•Sicher•BSI•

Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung

Version 1.0
Vom 26.09.2022

CYBERIA

CTI

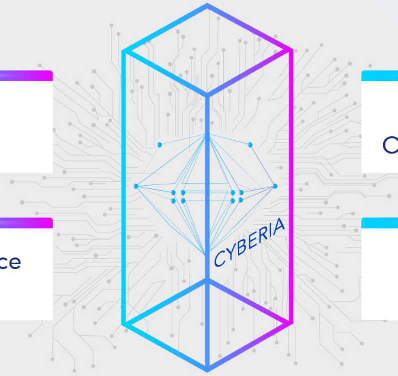
Alarmierung

Automatisiert neutralisieren (Echtzeit)

Automatisiert Berichten

TEHTRIS XDR AI PLATFORM

- Unified Console
- Advanced Analytics
- Threat Intel
- Sandboxes
- Threat Hunting
- Compliance Audits



- SOAR Orchestration
- Response Workflow
- Artificial Intelligence
- UEBA
- APIs
- Ticketing System

- XDR EDR OPTIMUS
- XDR MTD
- XDR SIEM
- XDR NTA
- XDR Honeypots Deceptive Response
- XDR CYBERIA eGuardian

- XDR Zero Trust
- XDR Email Protection
- XDR Identity Access Management

TECHNICAL LANDSCAPE

CLOUD

aws	Azure
Google Cloud	OVH

SYSTEMS

Endpoints	Servers
Mobile	IoT

NETWORKS

SD-Wan	Firewalls
VPN	Network flows

/03

Mehrwerte

Zentrale holistische Lösung zur IT-/OT-Security

Mehrwerte:

Zentralisierte Analyse und Reaktion auf Sicherheitsereignissen in einer Oberfläche

24/7 Threat Monitoring, & XDR / EDR Konfiguration

Managed Service spart eigne Ressourcen

Zentrale holistische Lösung zur IT-/OT-Security

Mehrwerte Compliance:

ISO27001:2022
Anhang A
5.7 Erkenntnisse über Bedrohungen
5.9 Inventarisierung
5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse
5.26 Reaktion auf Informationssicherheitsereignisse
5.27 Erkenntnisse aus Informationssicherheitsereignisse
5.28 Sammeln von Beweismitteln
8.1 Schutz von Endpoints
8.7 Schutz vor Schadcode
8.8 Handhabung von technischen Schwachstellen
8.9 Konfigurationsmanagement
8.12 Verhinderung von Datenlecks
8.15 Protokollierung
8.16 Überwachung von Aktivitäten
8.19 Installation von Software auf Systemen im Betrieb
8.23 Webfilterung
8.23 Änderungssteuerung

Zentrale holistische Lösung zur IT-/OT-Security

Mehrwerte Compliance:

BSI KRITIS 2.0 / SZA (System zur Angriffserkennung)

B3S

TISAX

NIS 2 Maßnahmen

…

TEHTRIS SZA Lösung

Unser europäischer Lösungsansatz für die Anforderungen der BSI OH SZA mit der TEHTRIS XDR Plattform

NICO RIEGER

mt

e Dienstleistungen zu sichern in dem wir Angriffe
atisiert in Echtzeit neutralisieren.

Nachweis für <Stufe 5> zu erbringen. Sie
alisiert sicherheitsrelevante Ereignisse in Echtzeit in

en, die dabei helfen, Endpoint-Security,
entralen Punkt durchzuführen.

ategorien MUSS, SOLL und KANN formuliert. Wir
hlen, sowie beschrieben, wie diese Module Sie im

Security-Produkte (Dritthersteller) an die XDR-

itsaudits bei KRITIS-Betreibern

- limited - 1

n Systeme zur Angriffserkennung

Maßnahmenart (MUSS / SOLLTE / KANN)	Welches Modul(e) unterstützt Sie bei der Erfüllung	Beschreibungen, wie Ihnen die Lösungen von TEHTRIS bei der Erfüllung der Anforderungen helfen.
GRUNDLEGENDES		
Muss	XDR, EDR, EPP, MTD, NTA, …	TEHTRIS bietet eine Plattform und Module, um ein ganzheitliches IT-/OT-/MT-Sicherheitskonzept umzusetzen.
Muss	XDR, EPP, EDR, NTA, CTI	Unsere XDR-Plattform ermöglicht die Suche nach bekannten CVEs. Mit unserer CTI erhalten Sie aktuelle, lokale und branchenspezifische Cyberbedrohungsdaten, die Sie mit unseren Modulen erkennen und blockieren können. Zusätzlich verfügt unser EDR-Modul über einen Vulnerability Scanner.
Muss	CTI und 24/7 Support nach dem Follow the Sun Prinzip	Unsere Forschungs- und Entwicklungsabteilung sowie unser SOC sorgen rund um die Uhr für einen zuverlässigen Betrieb der XDR-Plattform, einschließlich des Update-Services. Secure by Design: - Jedes Produkt läuft auf dem gehärteten TEHTRIX-Betriebssystem mit vollständiger Festplattenverschlüsselung, RBAC und Anti-0-Day-Schutz. - TEHTRIS EDR kann selbst mit Administratorrechten nicht deinstalliert werden (Treiber auf Kernel-Ebene signiert). - Datenflüsse sind verschlüsselt (TLS 1.3).

MUSS.

- limited - 2

Zentrale holistische Lösung zur IT-/OT-Security

Abschließende Tips:

Achten Sie auch bei der Auswahl Ihrer Produkte und Dienstleister auf Sicherheit.

MDR und SOC sind schöne Marketingbegriffe. Achten Sie auf die Inhalte.

Setzen Sie Security-Lösungen ein, um Ihre Infrastruktur zu schützen und nicht nur um Vorschriften zu erfüllen.

TEHTRIS DNA => SECURITY & PRIVACY by DESIGN

Secure by Design

Jedes Produkt läuft auf dem gehärteten TEHTRIX-Betriebssystem mit vollständiger Festplattenverschlüsselung, RBAC, Anti-0-Day-Schutz

TEHTRIS EDR kann auch mit Administratorrechten nicht deinstalliert werden (Treiber auf Kernel-Ebene signiert)

Verschlüsselte Kommunikation (TLS 1.3)

Schutz von geistigem Eigentum

Unterliegt nicht dem US Cloud Act

Unsere Lösungen können und müssen nicht auf den Inhalt Ihrer Dateien zugreifen, um Ihr Informationssystem zu schützen (keine Remote Shell)

Hash- und/oder Binärabfragen an externe CTI-Feeds sind privat und anonym

Bei On-Prem-VMs bleiben die Rohdaten vor Ort

Datenschutz

100% konform mit der EU GDPR, einer der restriktivsten Vorschriften

Daten werden in einer privaten, sicheren Cloud auf kundenspezifischen Rechnern gehostet

Schutz des Informationssystems bei gleichzeitiger Erfassung und Verarbeitung der geringstmöglichen Menge an personenbezogenen Daten

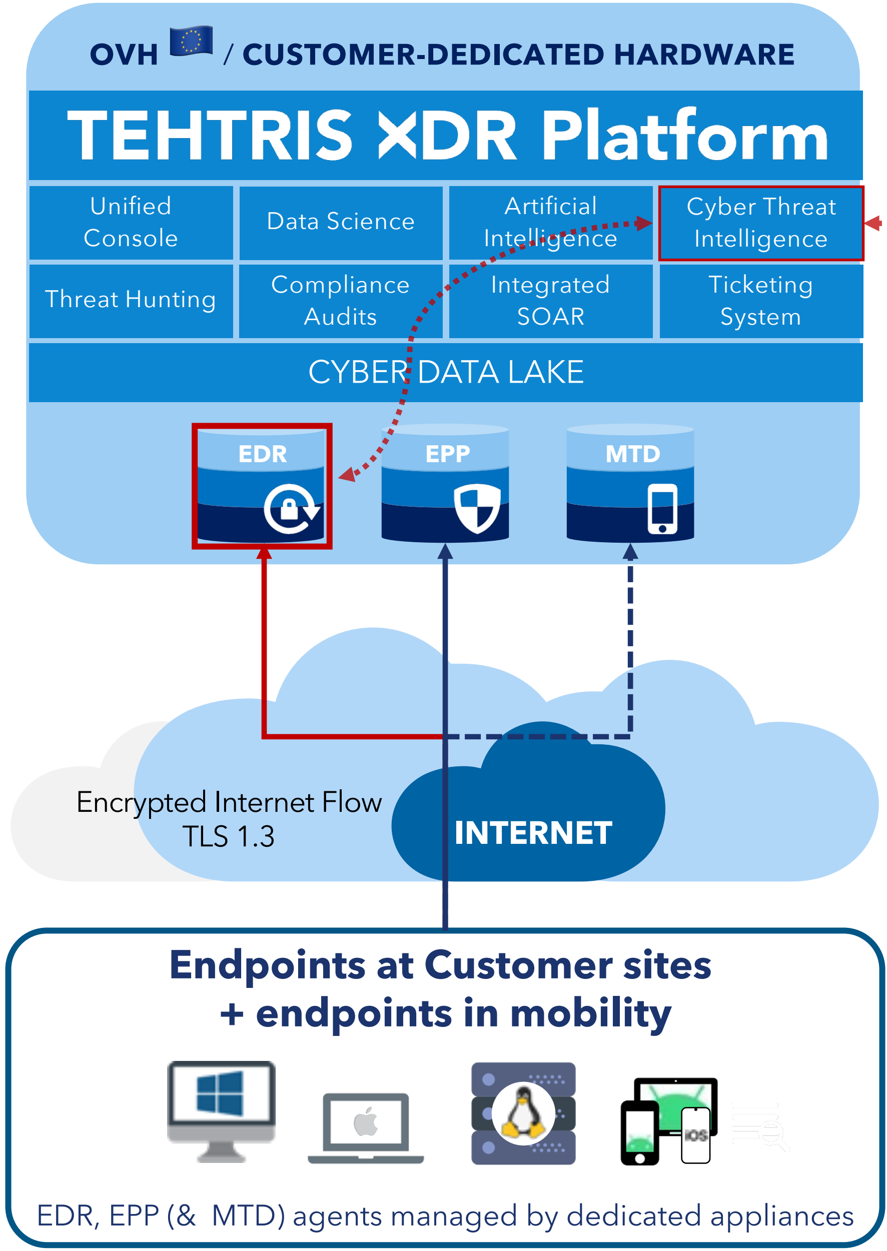
DATA FLOW

Binaries hashes flow analysis
(detailed on the next slide)

VPN

Customer environment

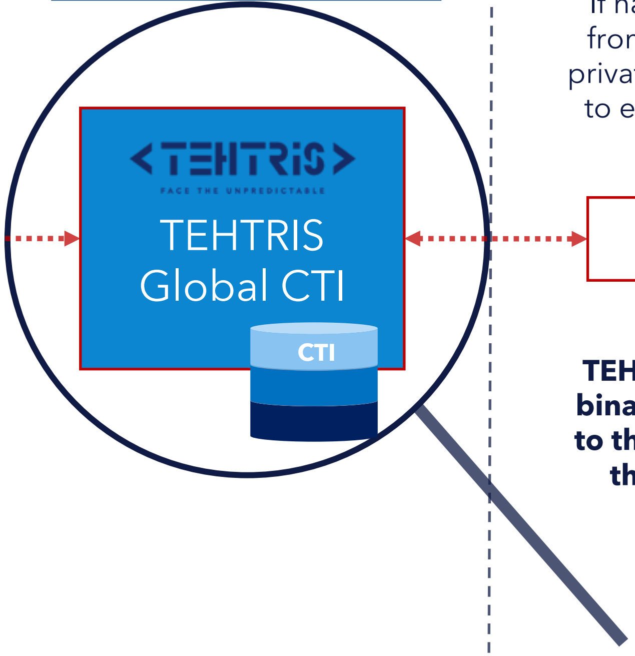
SIEM is not represented in this picture



Endpoints at Customer sites + endpoints in mobility

EDR, EPP (& MTD) agents managed by dedicated appliances

Zoom on TEHTRIS CTI



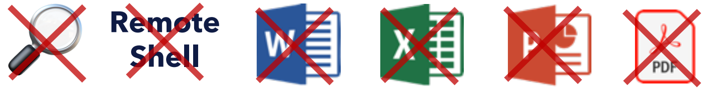
External sources

If hashs are unkown from TEHTRIS CTI, a private request is done to external database

External CTI feeds

TEHTRIS never sends binary files belonging to the customer out of the TEHTRIS XDR platform

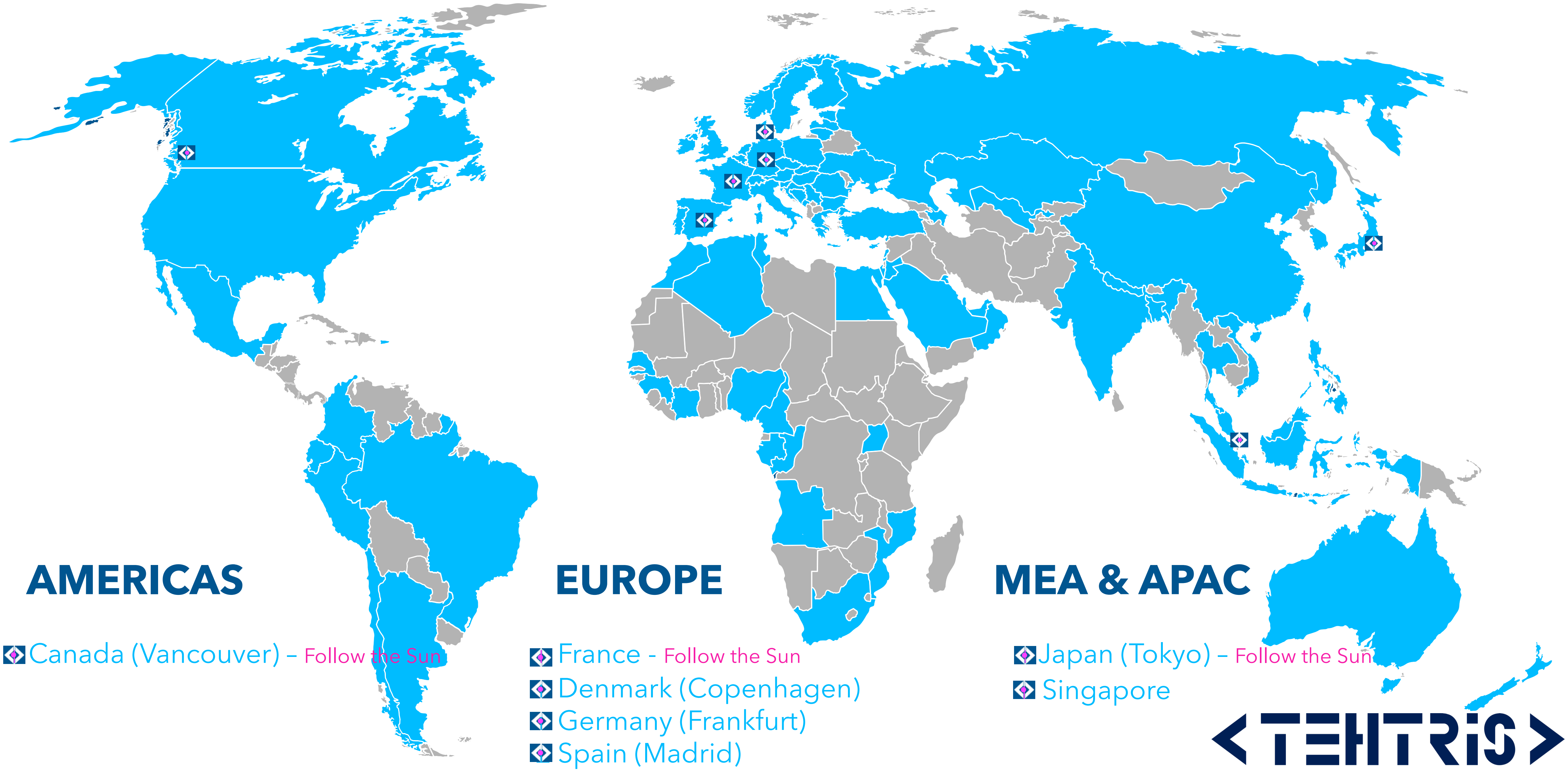
TEHTRIS products do not allow the opening or access to ANY customer file, unlike other competitors.



100% native technology with hosting.

Only EU jurisdiction will apply

TEHTRIS WORLDWIDE



AMERICAS

- Canada (Vancouver) – Follow the Sun

EUROPE

- France - Follow the Sun
- Denmark (Copenhagen)
- Germany (Frankfurt)
- Spain (Madrid)

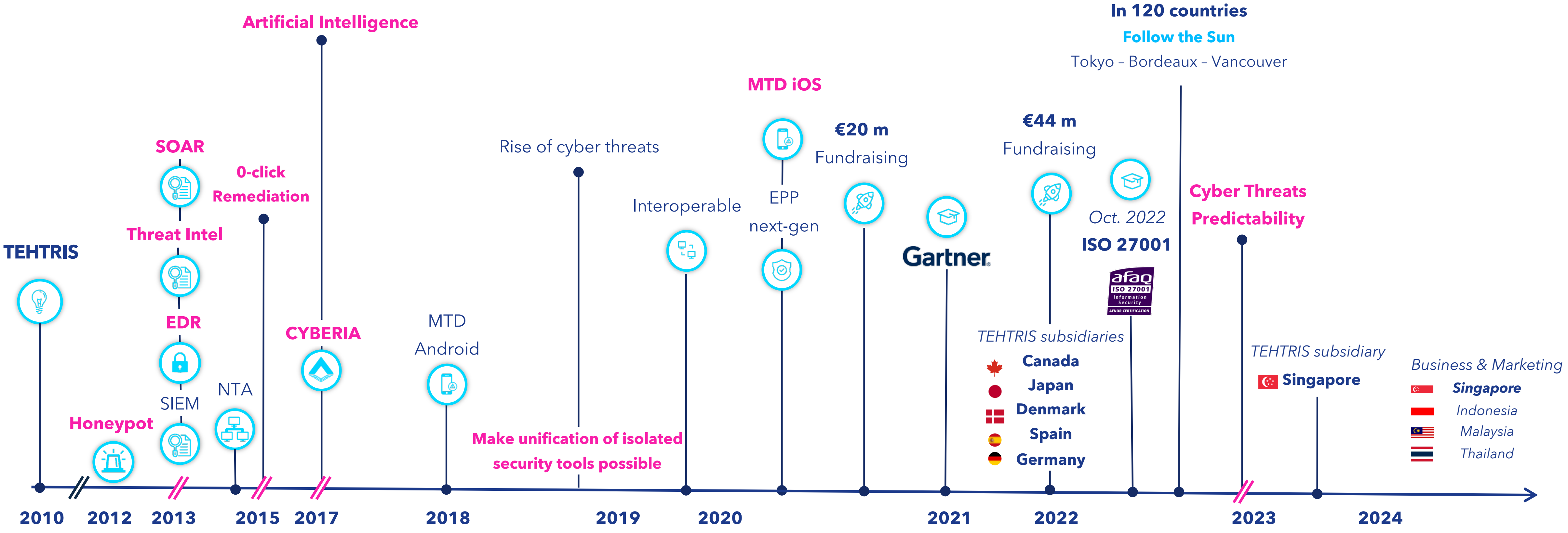
MEA & APAC

- Japan (Tokyo) – Follow the Sun
- Singapore

<TEHTRIS>
FACE THE UNPREDICTABLE

TEHTRIS XDR AI PLATFORM

Pioneering innovation: Setting standards years ahead of competitors



TEHTRIS

2010

Honeypot

2012

SOAR

Threat Intel

EDR

SIEM

2013

NTA

0-click Remediation

2015

Artificial Intelligence

CYBERIA

2017

MTD Android

2018

Rise of cyber threats

Make unification of isolated security tools possible

2019

Interoperable

2020

MTD iOS

EPP next-gen

€20 m Fundraising

Gartner

2021

€44 m Fundraising

TEHTRIS subsidiaries

Canada

Japan

Denmark

Spain

Germany

2022

Oct. 2022

ISO 27001

afaq ISO 27001 Information Security AFNOR CERTIFICATION

In 120 countries

Follow the Sun

Tokyo – Bordeaux – Vancouver

Cyber Threats Predictability

2023

TEHTRIS subsidiary

Singapore

Business & Marketing

Singapore

Indonesia

Malaysia

Thailand

2024

Private and public customers, from SMEs to large organizations (+200k endpoints)

Zusammenfassung

Unsere **TEHTRIS XDR-Plattform** ist die **Sicherheitslösung** zur Bekämpfung von **Spionage** und **Sabotage**.

Sie bietet einen **ganzheitlichen Überblick** über die geschützten IT-/OT-Systeme und eine **automatisierte Echtzeit-Verteidigung** gegen alle bekannten und unbekannten Angriffe, um die Verfügbarkeit der Infrastrukturen zu gewährleisten.

MERCI !

THANK YOU !

Contact us!

Nico.Rieger@tehtris.eu

+49 151 200 23 903

TEHTRIS

FACE THE UNPREDICTABLE

Managed Industrial Security Services

Risikominimierung durch OT Managed Industrial Security Services

18. April 2024

Baldur Scherabon

Industrial System Cybersecurity Manager

baldur.scherabon@orangecyberdefense.com

Götz Weinmann

Senior Business Development Manager

goetz.weinmann@orangecyberdefense.com

orange Cyberdefense

Nice to meet you!

We are the leading security services provider, supporting your business globally.

€1.1 billion
turnover
in 2023.
+11% YoY

Over 3,000
multi-skilled cybersecurity experts.

+8,800
customers worldwide,
best in class in all verticals.

In-house CERT

400+
sources continuously feed into our threat intelligence datalake.

250+
experts dedicated to R&D and threat research.

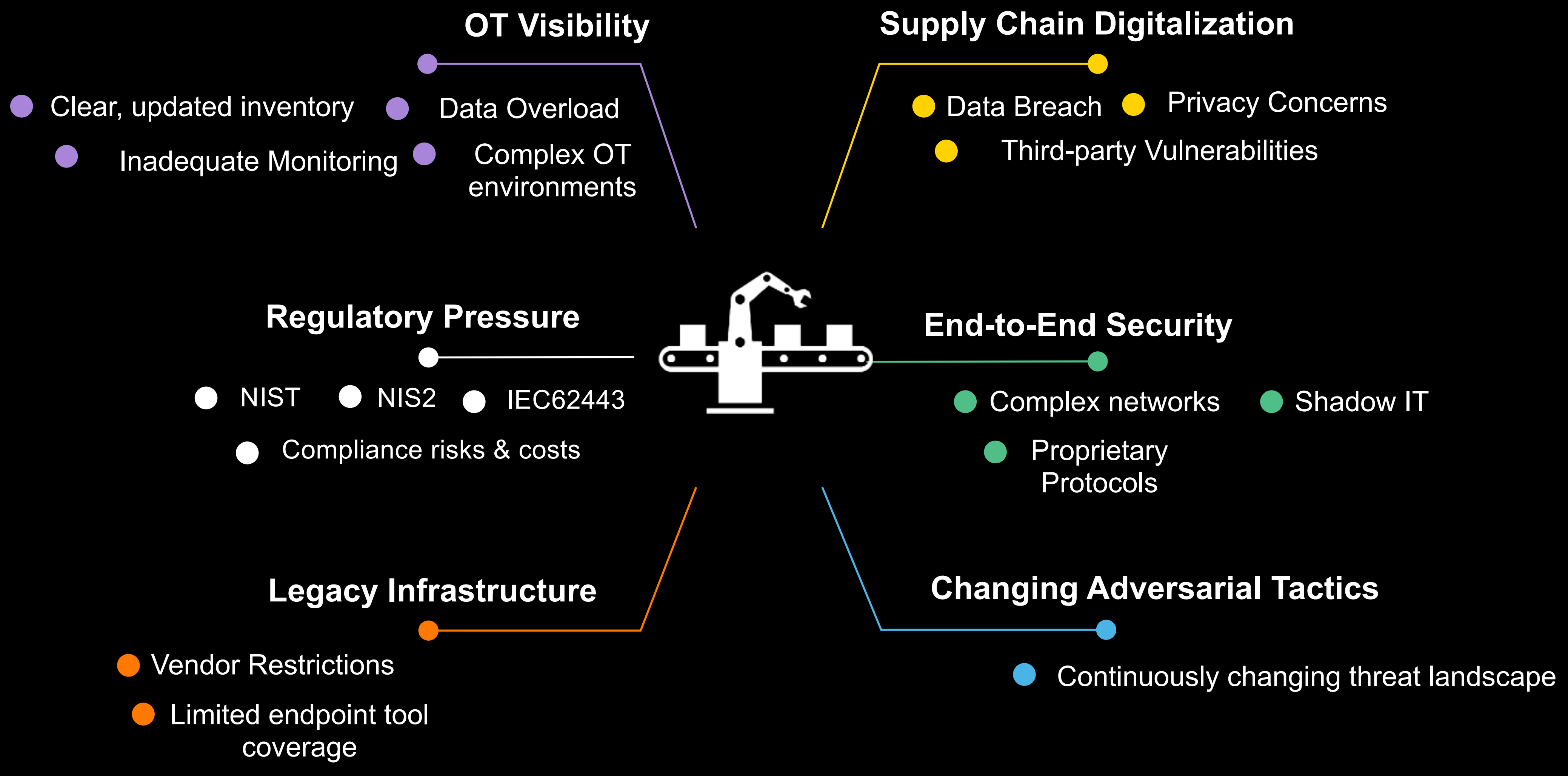
TF-CSIRT
Trusted Introducer

FIRST

CREST

24/7/365
continuous monitoring of security systems worldwide.

Cybersecurity is a journey, not a destination



OT Visibility

- Clear, updated inventory
- Data Overload
- Inadequate Monitoring
- Complex OT environments

Supply Chain Digitalization

- Data Breach
- Privacy Concerns
- Third-party Vulnerabilities

Regulatory Pressure

- NIST
- NIS2
- IEC62443
- Compliance risks & costs

End-to-End Security

- Complex networks
- Shadow IT
- Proprietary Protocols

Legacy Infrastructure

- Vendor Restrictions
- Limited endpoint tool coverage

Changing Adversarial Tactics

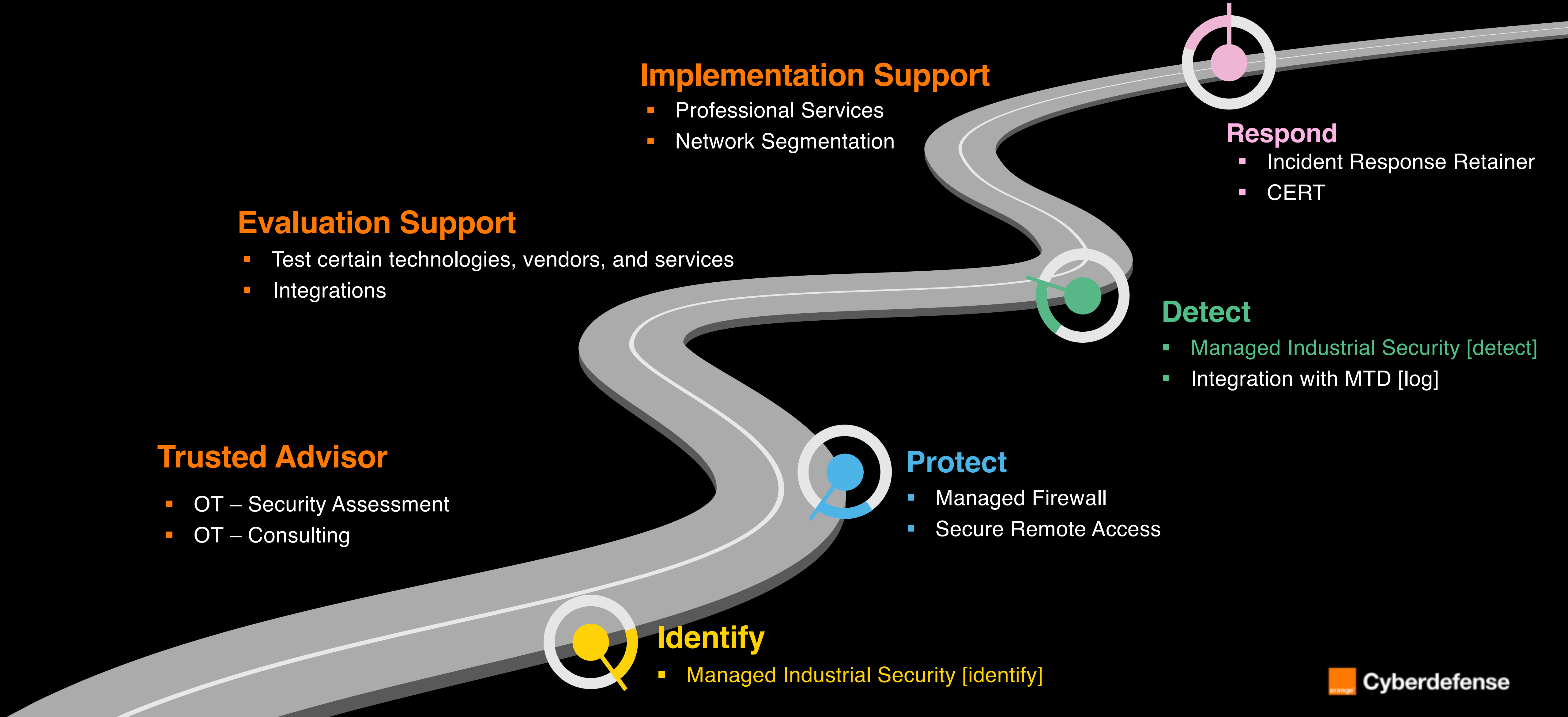
- Continuously changing threat landscape

So many value-creating challenges, but they are creating new vulnerabilities.

Types of OT cyber attacks

Category	1 IT TTPs			2 OT TTPs	
Type	1a	1b	1c	2a	2b
	IT targeted	IT/OT targeted	OT targeted	OT targeted, crude	OT targeted, sophisticated
Characteristics	IT attacked; production impacted indirectly as collateral damage	IT attacked, Windows/Linux-based OT attacked with IT TTPs directly or as collateral	Windows/Linux-based OT attacked with IT TTPs directly	Dedicated OT devices attacked with OT-specific TTPs crudely, little precision or complexity	Dedicated OT devices attacked with OT-specific TTPs with sophistication

OT Security Journey



Trusted Advisor

- OT – Security Assessment
- OT – Consulting

Evaluation Support

- Test certain technologies, vendors, and services
- Integrations

Implementation Support

- Professional Services
- Network Segmentation

Identify

- Managed Industrial Security [identify]

Protect

- Managed Firewall
- Secure Remote Access

Detect

- Managed Industrial Security [detect]
- Integration with MTD [log]

Respond

- Incident Response Retainer
- CERT

24x7 Platform Management

Asset Information Management

Prioritized recommendations and reporting

[identify]

Managed Industrial Security Services

[detect]

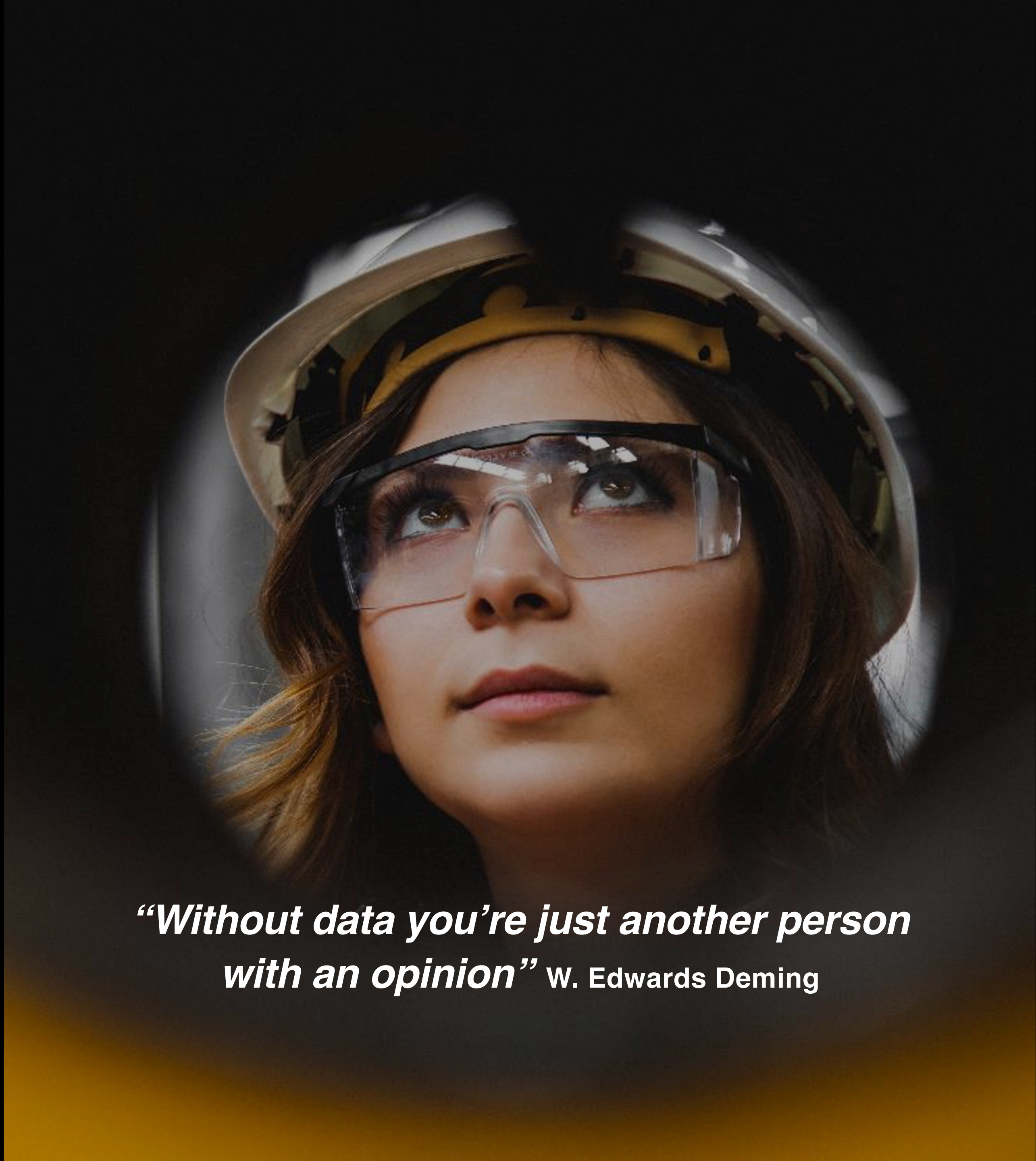
Threat Detection

24x7 Security Incident Analysis & Response

24x7 Platform Management

You can’t protect what you don’t know.

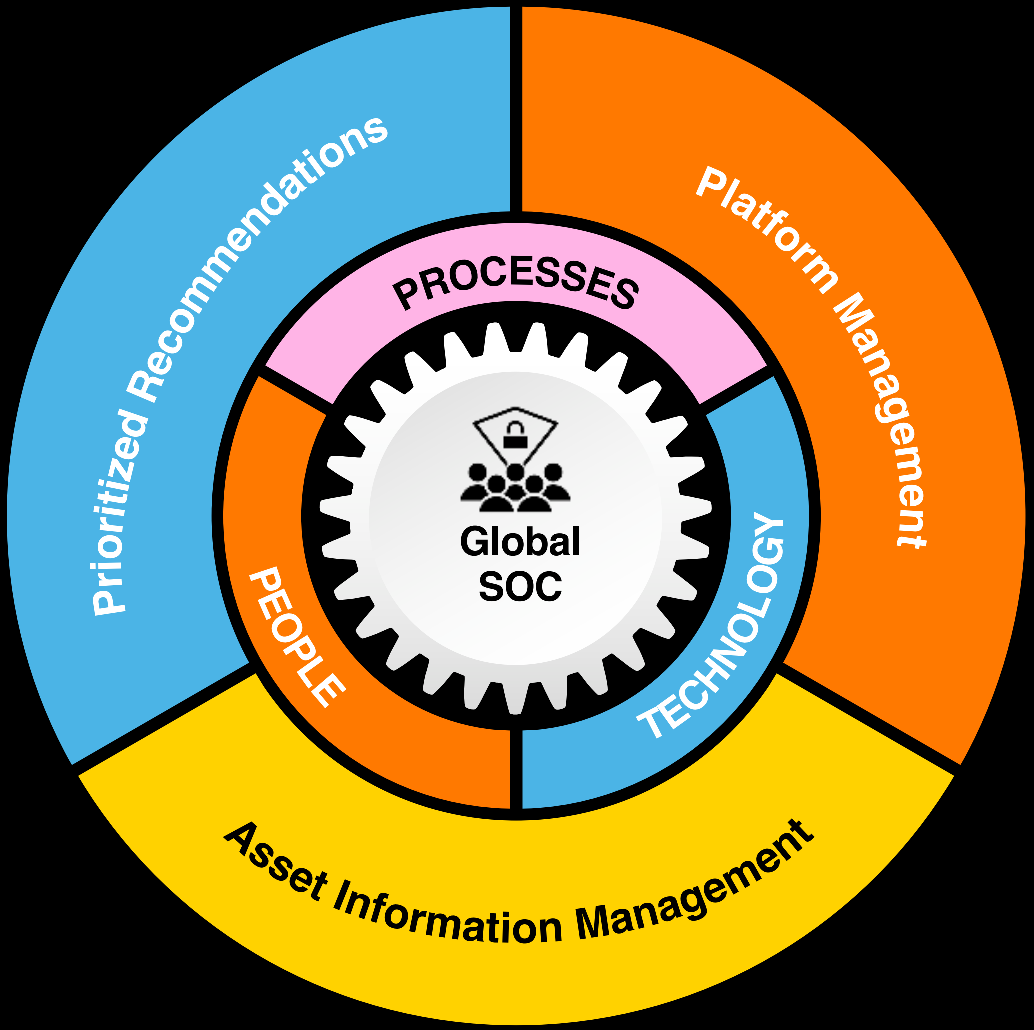
Get visibility for data driven OT security.



“Without data you’re just another person with an opinion” W. Edwards Deming

Managed Industrial Security [identify]

Turning visibility in data driven OT security.



Vendor Agnostic Approach

Orange Cyberdefense service platform to support different vendors and deployment types.

Platform Management

24x7 operations of your OT Security Platform.

Asset Information Management

Building and maintaining an asset inventory with contextualized data to support your risk-based decision making.

Prioritized Recommendations

Providing actionable recommendation specific to your OT environment and early warnings on new vulnerabilities.

Managed Industrial Security [identify]
Visibility – Asset Information Management

Orange Cyberdefense Portal

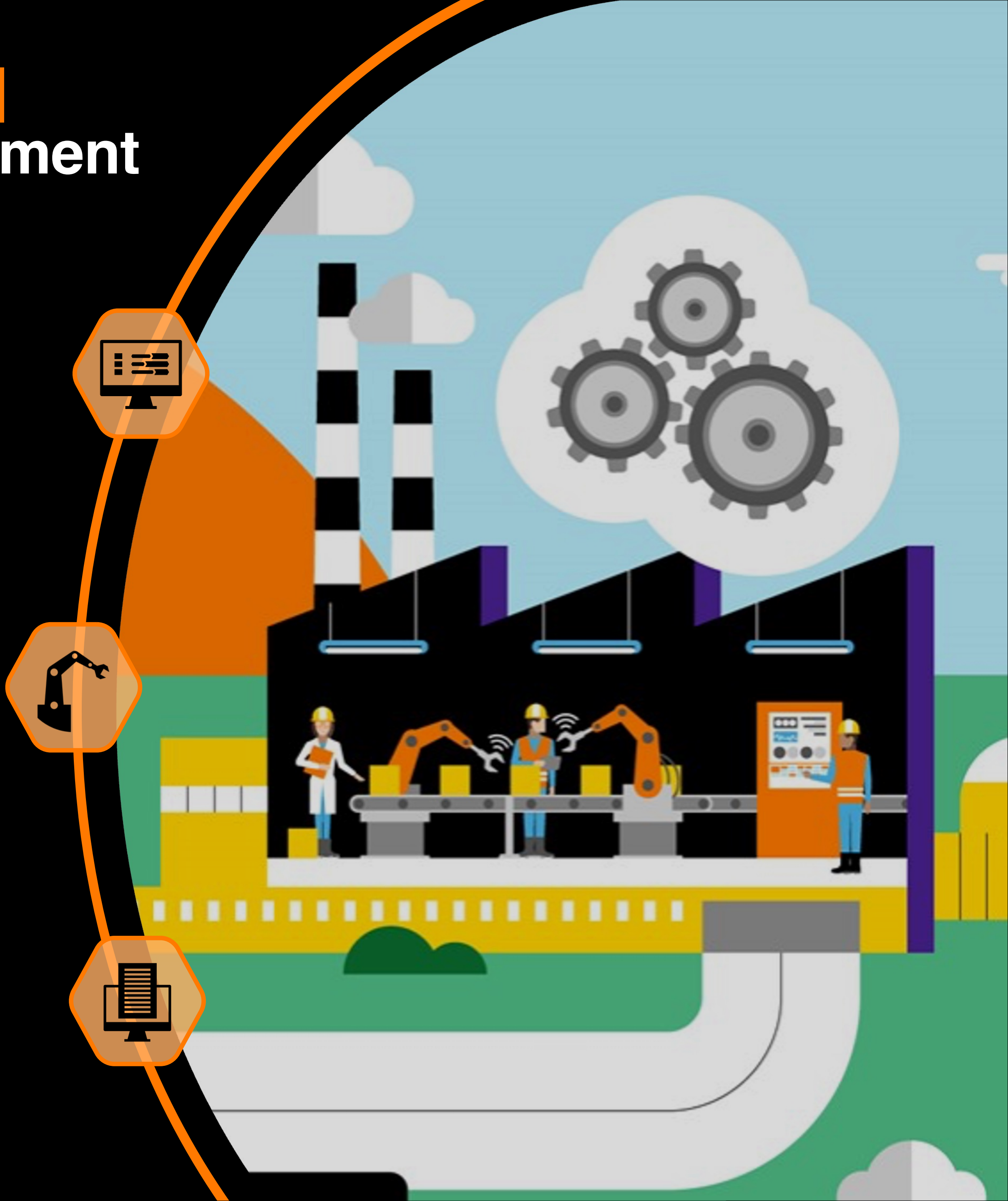
- ✓ Pre-defined dashboards
- ✓ Customization of dashboards to your needs
- ✓ Full access to your asset information

Asset Inventory Management

- ✓ Keeping your asset information up-to-date and relevant
- ✓ Contextualization of asset information
- ✓ Mapping of connections and vulnerabilities with assets
- ✓ Change and enrichment of asset information

Reporting & Notification

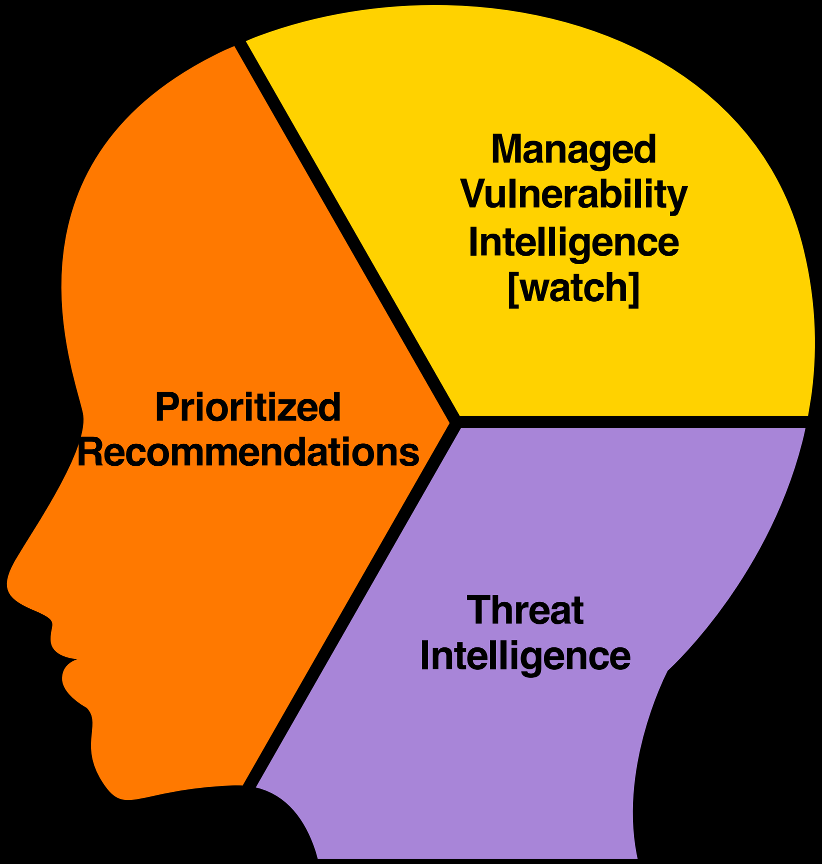
- ✓ Monthly strategic report on OT assets
- ✓ Notification of critical vulnerabilities on OT assets



Managed Industrial Security [identify]
Focus – Prioritized Recommendations & Vulnerability Alerts

Prioritized Recommendations

- ✓ Review of your OT asst information by OT experts
- ✓ Providing actionable recommendations specific to your OT environment
- ✓ Continuously increase your security maturity
- ✓ Monthly recommendation report


Managed Vulnerability Intelligence [watch]
Prioritized Recommendations
Threat Intelligence

Managed Vulnerability Intelligence [watch]

- ✓ Vulnerability Monitoring of OT products by the Orange Cyberdefense CERT
- ✓ Information about the latest vulnerabilities of OT products and the patches to be applied
- ✓ Early warnings of vulnerabilities on OT products as bulletin and security recommendations

Threat Intelligence

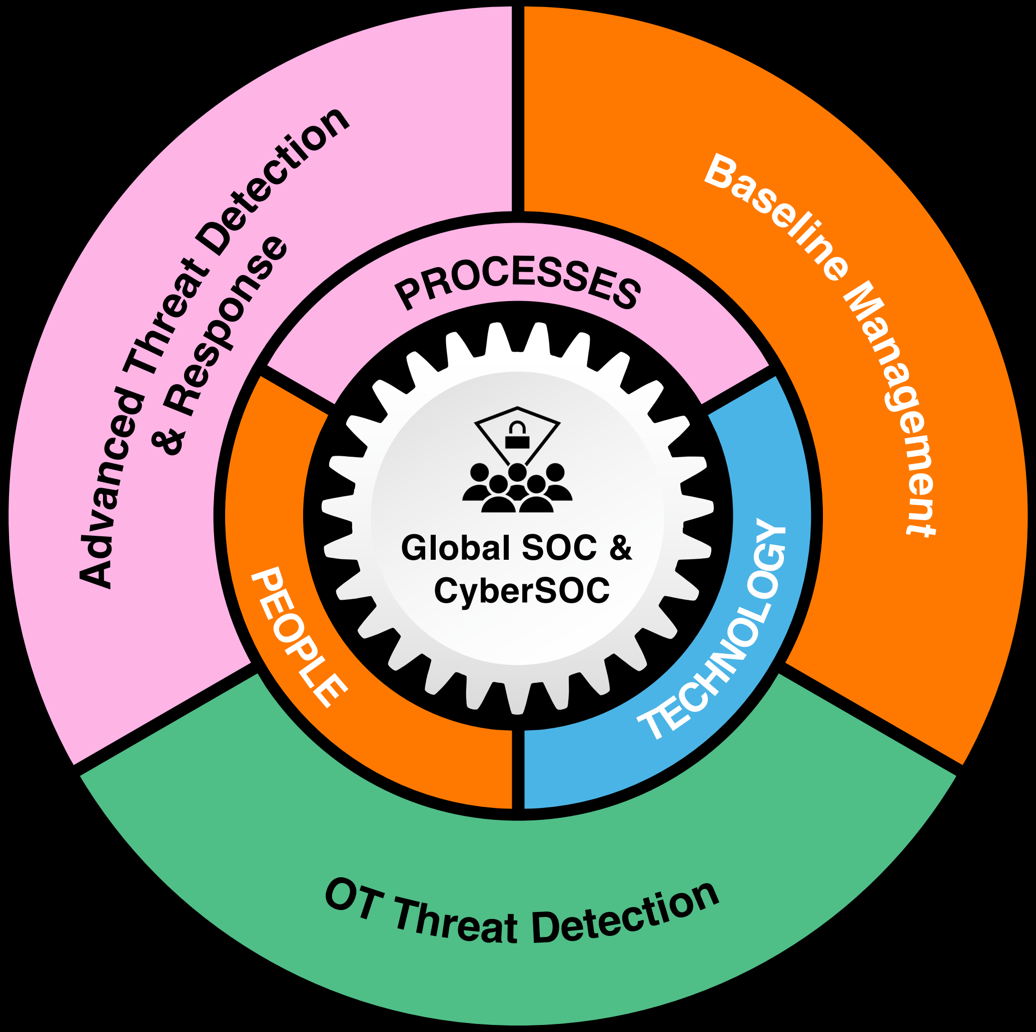
- ✓ Access to World Watch for daily threat advisories
- ✓ Enrichment of Asset Information with OT threat intelligence

Reducing risks and protecting sensitive data.

Extending Threat Detection to OT.

Managed Industrial Security [detect]

Reducing the operational risks of IT/OT connectivity.



Vendor Agnostic Approach

Orange Cyberdefense service platform to support different vendors and deployment types.

Baseline Management

Creation and management of a baseline and policies of your operational environment to detect threats and anomalies.

OT Threat Detection

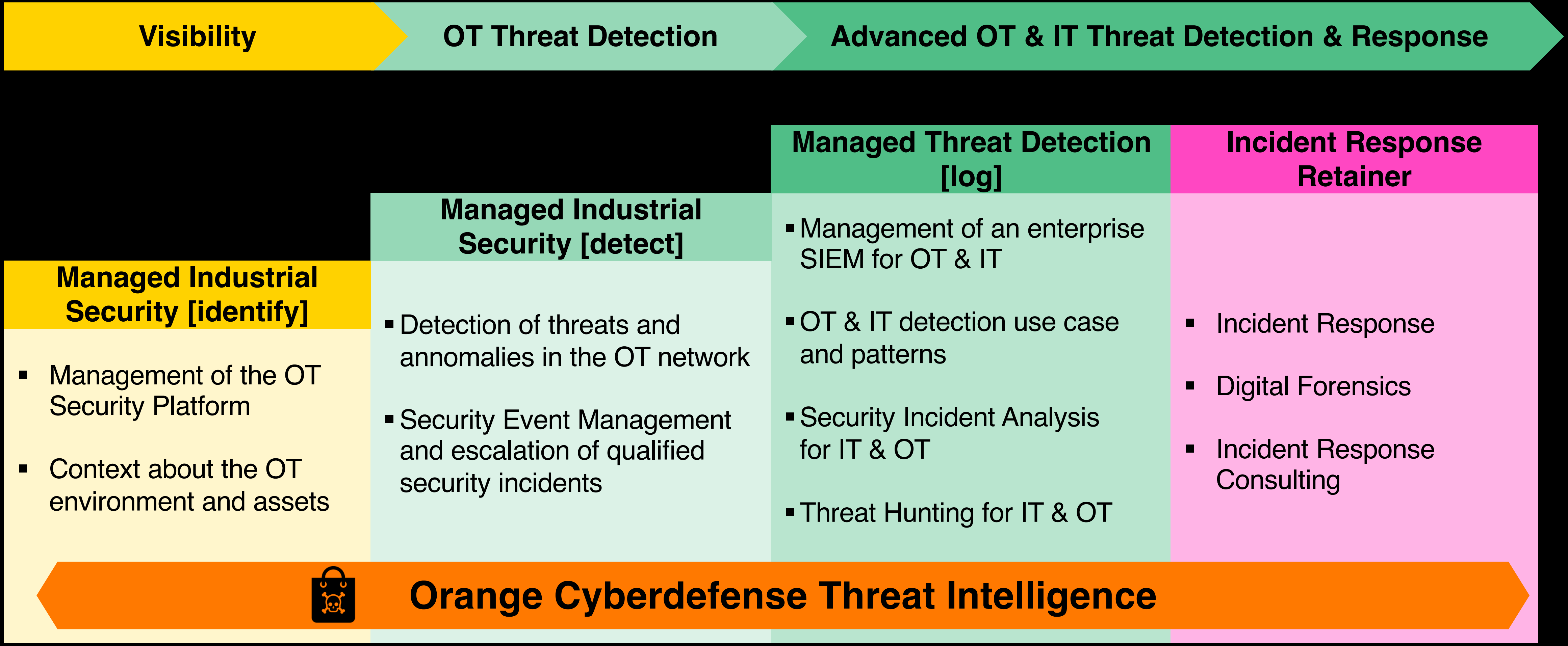
Detection and investigation of OT threats and escalation of qualified OT security incidents for collaborative response by dedicated OT specialists.

Advanced IT & OT Threat Detection & Response

Advanced detection and investigation of IT and OT threats, proactive hunting of threats and incident response.

Managed Industrial Security [detect]

Advanced OT & IT Threat Detection



Visibility → OT Threat Detection → Advanced OT & IT Threat Detection & Response

Managed Industrial Security [identify]

- Management of the OT Security Platform
- Context about the OT environment and assets

Managed Industrial Security [detect]

- Detection of threats and annomalies in the OT network
- Security Event Management and escalation of qualified security incidents

Managed Threat Detection [log]

- Management of an enterprise SIEM for OT & IT
- OT & IT detection use case and patterns
- Security Incident Analysis for IT & OT
- Threat Hunting for IT & OT

Incident Response Retainer

- Incident Response
- Digital Forensics
- Incident Response Consulting

Orange Cyberdefense Threat Intelligence

Monitoring & Protecting of global industrial environments

Requirements

- Managed OT Security Platform to gain an accurate inventory of the industrial environment
- OT network and connection mapping to enable segmentation activities
- Integration with customer CMDB
- Integration with customer OT/IT SOC and SIEM

Solution

- **Managed Industrial Security [identify]** service for continuous identification of assets and vulnerabilities
- **Managed Industrial Security [detect]** service for detection of threats in the OT environment
- Deployment of over 300 sensors for passive and active detection of connected OT- (and IT) assets
- Customer SOC integration and CMDB
- CMDB integration via API
- Security integrations to enrich OT device information

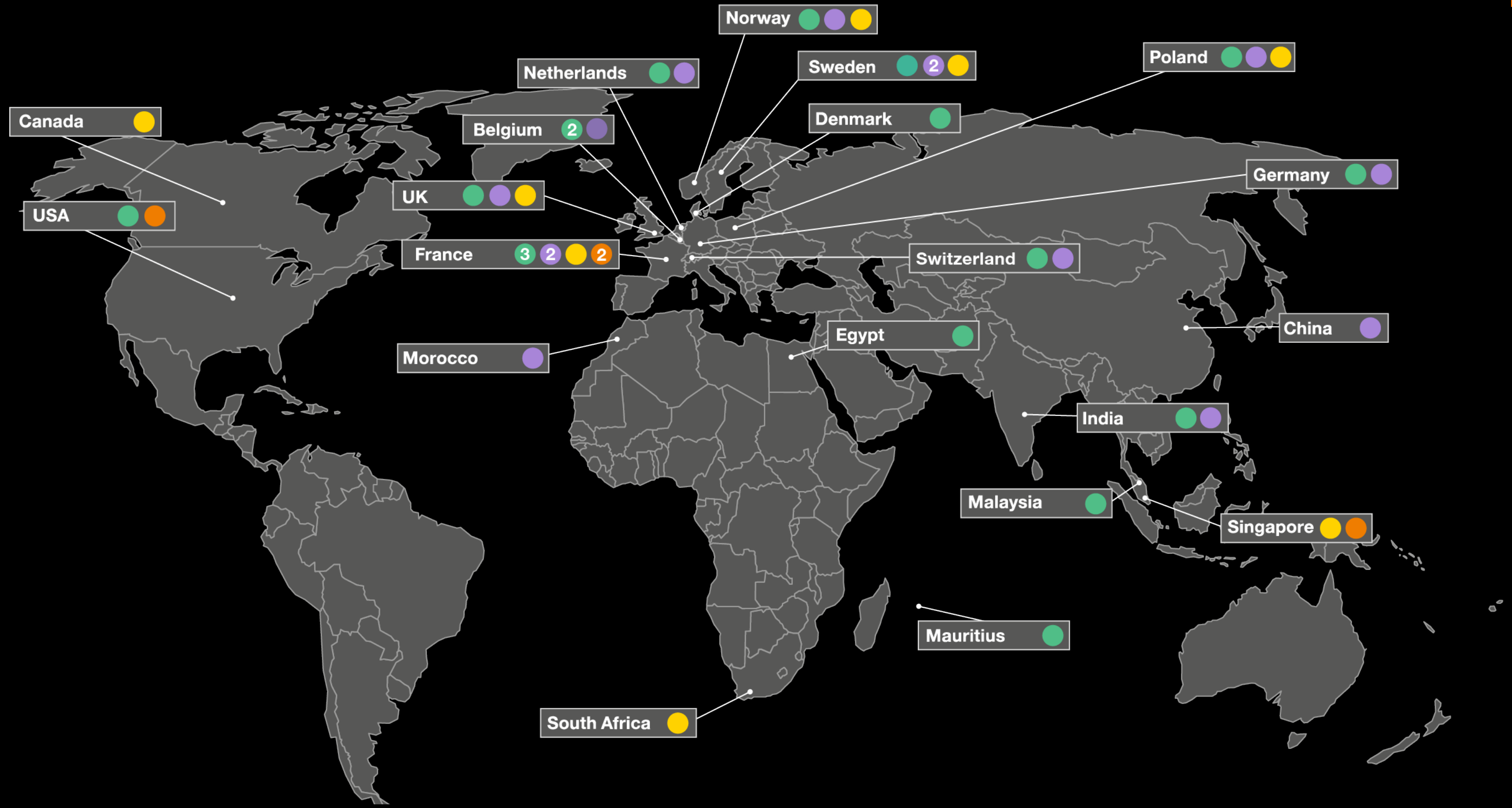
Customer profile

Industrial Products	38 000	8,8 billions	Germany 50 Countries

Benefits

- Collection of relevant data on OT assets to build a data driven security program
- Management of OT Security Platform with 300+ sensors
- Detection of threats and escalation of qualified incidents into the customer SOC
- Improved risk management for industrial environments
- Integration for OT Security process optimization
- Managed Industrial Security Services integration in customer SOC

European leader with global footprint and proven OT security expertise.



🟢 18 SOCs spread throughout the world monitor and respond to events 24/7/365

🟣 14 CyberSOCs that bring together the best expertise in threat analysis 24/7/365

🟡 CERT in 8 locations operating continuously

🟠 4 scrubbing centers to mitigate DDoS attacks

Why Orange Cyberdefense?

- End-to-end security solutions to secure the digital transformation of your business
- Dedicated OT security specialists
- Specialized OT managed security service delivery teams
- Cross-industry experience and know-how of industry standards
- Strong partnerships with market leading OT security vendors
- Recognized by Gartner in the OT Market Guide

BRIDGE IT & OT SECURITY EFFECTIVELY WITHIN A SOC – A REAL STORY

CyberCompare Summit

By Michael Shaw, Senior Sales Engineer

OBRELA

ESTABLISHED IN 2010

250+ CONTRACTS

250+ EMPLOYEES

20+ COUNTRIES

WE USE SECURITY ANALYTICS AND SOPHISTICATED RISK AND THREAT MANAGEMENT TECHNOLOGY TO DYNAMICALLY PROTECT OUR CLIENTS BY IDENTIFYING, ANALYZING, PREDICTING AND PREVENTING CYBER THREATS IN REAL TIME

OBRELA IN NUMBERS

OPERATIONAL METRICS 2023

14.5PBs
Logs Collected & Analyzed *

500K
Devices & Endpoints Monitored

12.3'
Actual Response Time * *

1.6M
Triaged Alerts Managed

99.9%
Availability SLA

20+
Countries

250+
Customers

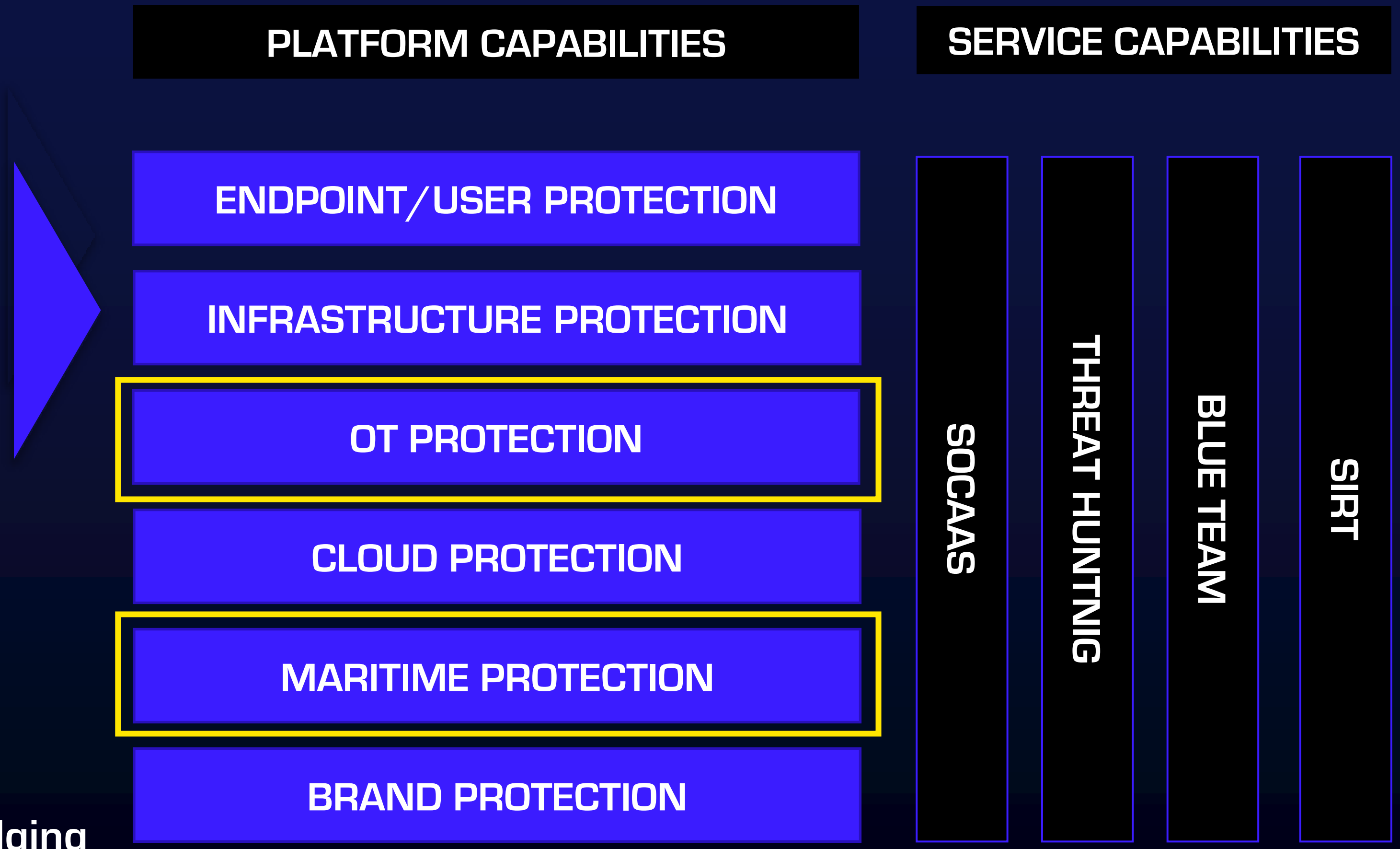
250+
Employees

* 2023 FIGURES YEAR TO DATE * *SLA

MDR

MANAGED DETECTION AND RESPONSE

One of the few MSSP providers bridging IT/OT to cover all your centralized and de-centralized assets into one dashboard for 24x7x365 coverage



PLATFORM CAPABILITIES

- ENDPOINT/USER PROTECTION
- INFRASTRUCTURE PROTECTION
- OT PROTECTION
- CLOUD PROTECTION
- MARITIME PROTECTION
- BRAND PROTECTION

SERVICE CAPABILITIES

- SOCAAS
- THREAT HUNTNIG
- BLUE TEAM
- SIRT

THE SECOPS OT CHALLENGE

GENERAL SECURITY OPERATIONS VS OT SECURITY OPERATIONS

SIEM Implementation

Insufficient Monitoring

Lack of Optimization & Tuning

No/Limited Automation of Response actions

Cost of Deployment & Ownership

VS

Data Types

Lack of OT and IoT Visibility

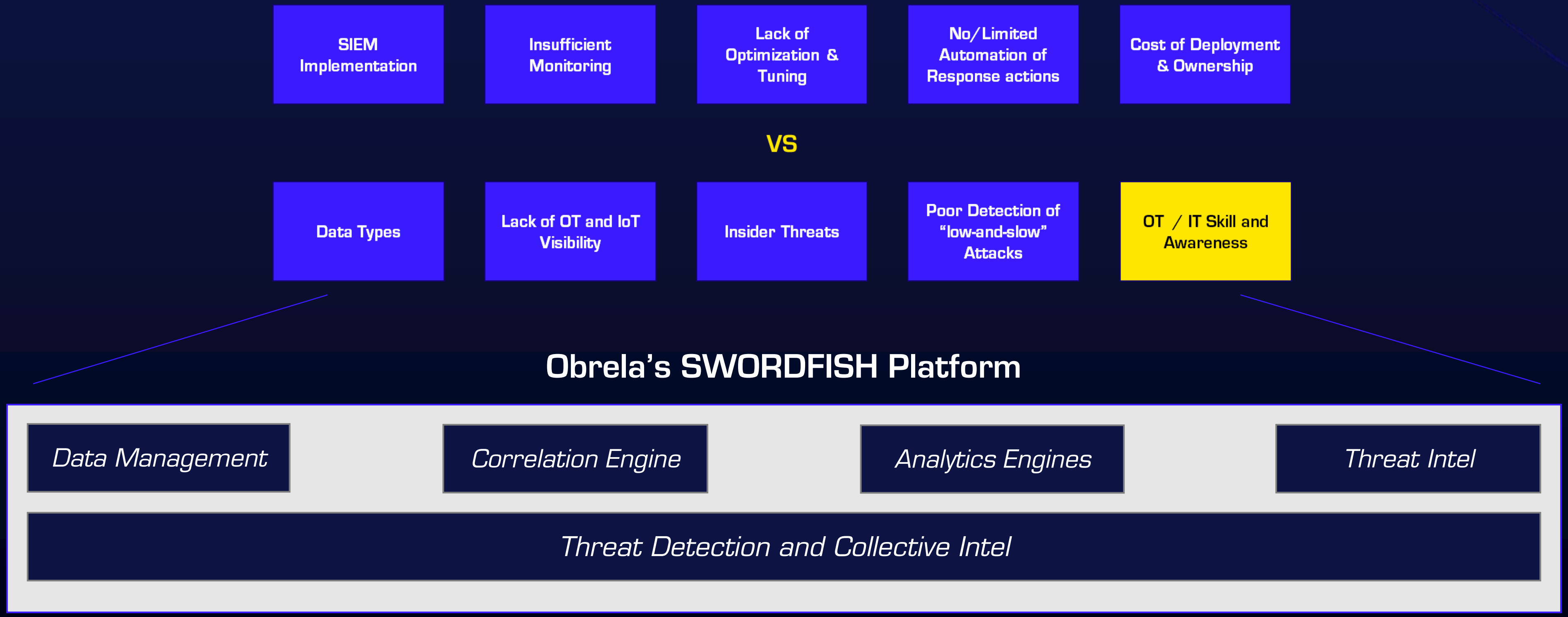
Insider Threats

Poor Detection of “low-and-slow” Attacks

OT / IT Skill and Awareness

THE SECOPS OT CHALLENGE

A PROPRIETARY MDR + COMPLIANCE PLATFORM



SIEM Implementation

Insufficient Monitoring

Lack of Optimization & Tuning

No/Limited Automation of Response actions

Cost of Deployment & Ownership

VS

Data Types

Lack of OT and IoT Visibility

Insider Threats

Poor Detection of "low-and-slow" Attacks

OT / IT Skill and Awareness

Obrela's SWORDFISH Platform

Data Management

Correlation Engine

Analytics Engines

Threat Intel

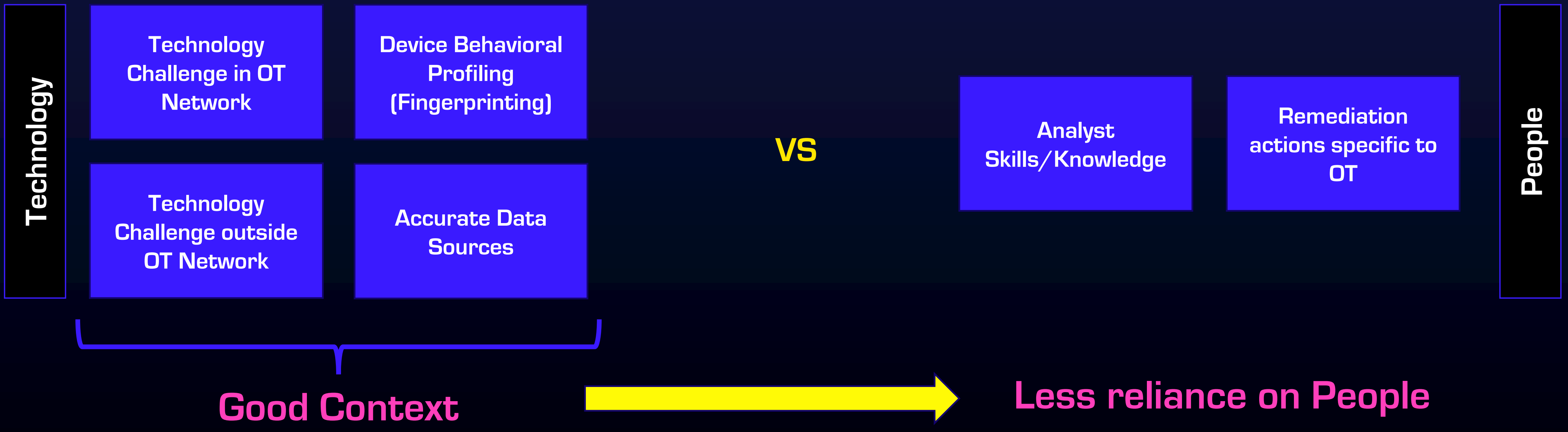
Threat Detection and Collective Intel

Single pane of glass, single interaction for all events/alerts of monitored devices, IT, OT, IOT, Maritime, Device and Vendor Agnostic

THE SECOPS OT CHALLENGE

Technology/Skills gap for OT? Is it real?

Short Answer – Yes.
But it is not as bad as you think…



Technology

Technology Challenge in OT Network

Device Behavioral Profiling (Fingerprinting)

Technology Challenge outside OT Network

Accurate Data Sources

VS

Analyst Skills/Knowledge

Remediation actions specific to OT

People

Good Context

Less reliance on People

GERMAN PHARMA COMPANY

Challenges/Business Objectives

Customer Challenges

Challenge #1

- *Customer was seeking a SIEM outcome which will perform the heart of a SOC to be delivered on a 24x7x365 basis.*

Challenge #2

- *Integrating OT telemetry with MDR tooling*
- *Correlation of IT and OT operations*

Challenge #3

- *No detection of threats within OT environment*

Challenge #4

- *User activity across IT and OT environments from a user context, not device context*

GERMAN PHARMA COMPANY

Solution Proposed

Technology + Operations + Services

Challenge #1

- *Customer sought a SIEM outcome which performs at the heart of a SOC to deliver to 24x7x365 basis.*

Obrela MDR Services:

- *24x7x365 Service Desk*
- *Full event/incident triage with Incident Response*
- *Based Customer's Sentinel – cheaper license costs*

Challenge #2

- *Integrating OT telemetry with MDR tooling*
- *Correlation of IT and OT operations*

Obrela MDR Integrations with:

- *Customer Sentinel*
- *Customer Defender for Cloud Apps*
- *24x7x365 Service Desk with single proprietary correlation engine - Swordfish*

Challenge #3

- *No detection of threats within OT environment*

Obrela MDR Services:

- *MDR Service includes pro-active Threat Hunting*
- *Obrela MDR for OT into Swordfish*

Challenge #4

- *User activity across IT and OT environments from a user context, not device context*

Obrela MDR Integrations:

- *Customer Defender for Identity integration into Swordfish*

GERMAN PHARMA COMPANY

Value Provided

Business Outcomes

- *Improved visibility of cloud resources for compliance and risk of information disclosure*
- *Customer received a full response capability including Blue Teaming recommendations*
- *Increased fidelity of alerts through Obrela HardCORE content using Lighthouse*
- *Lower false-positive rate through incorporation of user activity for threat detection*
- *Gave the customer peace of mind for uptime of service as Obrela has not experienced an outage for over 5 years*
- *Augmented customer security capability with support of Obrela team*

GERMAN PHARMA COMPANY

Key Insights

What does this Use Case outline?

- *A scalable cloud-based solution integrating the customers IT and OT environments*
- *Repeatable Solution*
- *Vendor agnostic approach supplied customer with future-proof changes in Vendor strategy*
- *Uptime commitment and security peace of mind*
- *Deliver SOCaaS fully integrated and leverage Sentinel and E5*
- *Solution proposed for RFP response – Very flexible*
- *Extremely rapid response time for Critical and High regardless of Event/Alert quantity*

OUR MISSION

WE KEEP YOUR BUSINESS IN BUSINESS

OBRELA

OBRELA

THANK YOU

London | Athens | Frankfurt | Dubai | Riyadh

www.obrela.com

Bridging IT and OT

Frameworks, scope and approaches

G.M.Bartel
Robert Bosch GmbH
18th April 2024

Bridging IT and OT
Agenda

01

Frameworks

How are industrial automation and control systems and their operation influenced?

02

ISMS and OT

How ISO 27001/2 and IEC62443-2-1 come together.

03

Approach

How to address resources via policies effectively and efficiently.

04

Field of Action

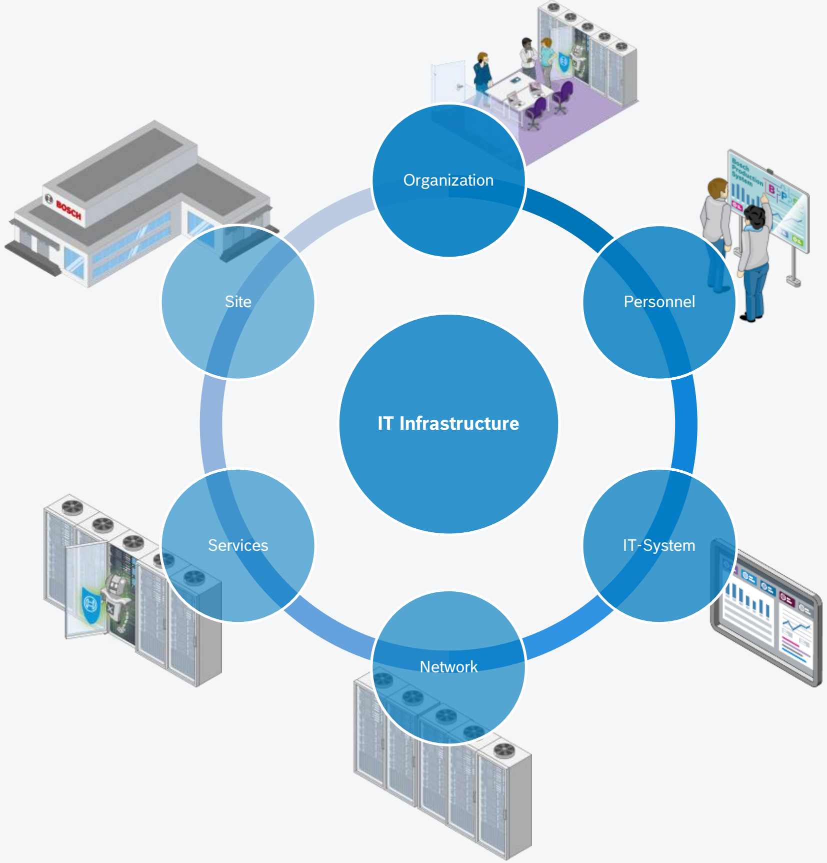
Ensure appropriate selection of solutions to tackle threats and vulnerabilities.

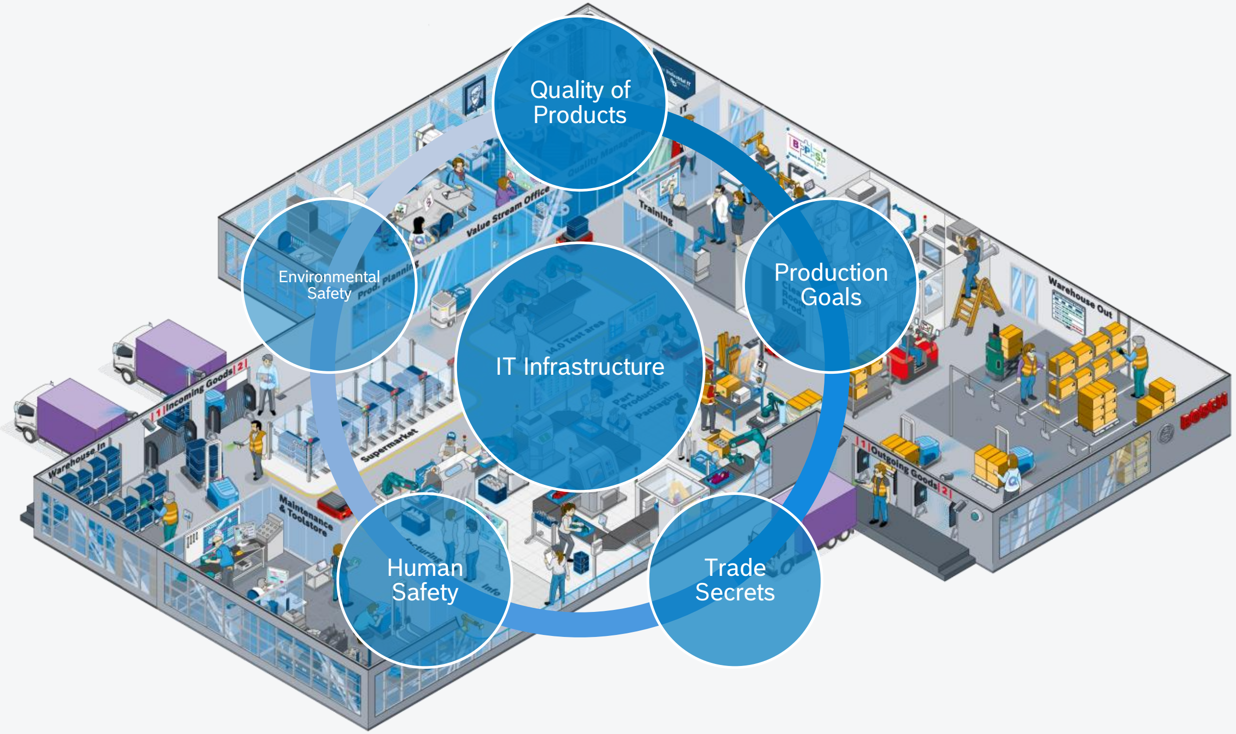
05

Wrap Up

5 take aways.

Bridging IT and OT
Introduction





Bridging IT and OT

IACS[1] as OT[2] compared with IT

Supporting Assets

Industrial Automation and Control Systems (IACS)

Description

Definition
Operational technology (OT[1]) is hardware and software that detects or causes a change, through the direct monitoring and/or control of **industrial equipment, assets, processes and events**. Such are often **proprietary** solutions operated in **isolated** environments.

Challenges / opportunities

- Decentral operation and heterogenic environment
- Specialized setups with "form follows function"
- IT/OT convergence blurring IT/OT distinction
- Time and cost driven environment with small numbers of clients

Primary target
OT environments in general must comply with strict **integrity, availability, and performance constraints** because operation outside of the constraints may impact health, safety, or the environment.

IT

Description

Definition
Information technology (IT) is a set of related fields that encompass **computer systems, software**, programming languages and **data and information** processing and storage. IT forms part of information and communications technology (ICT).

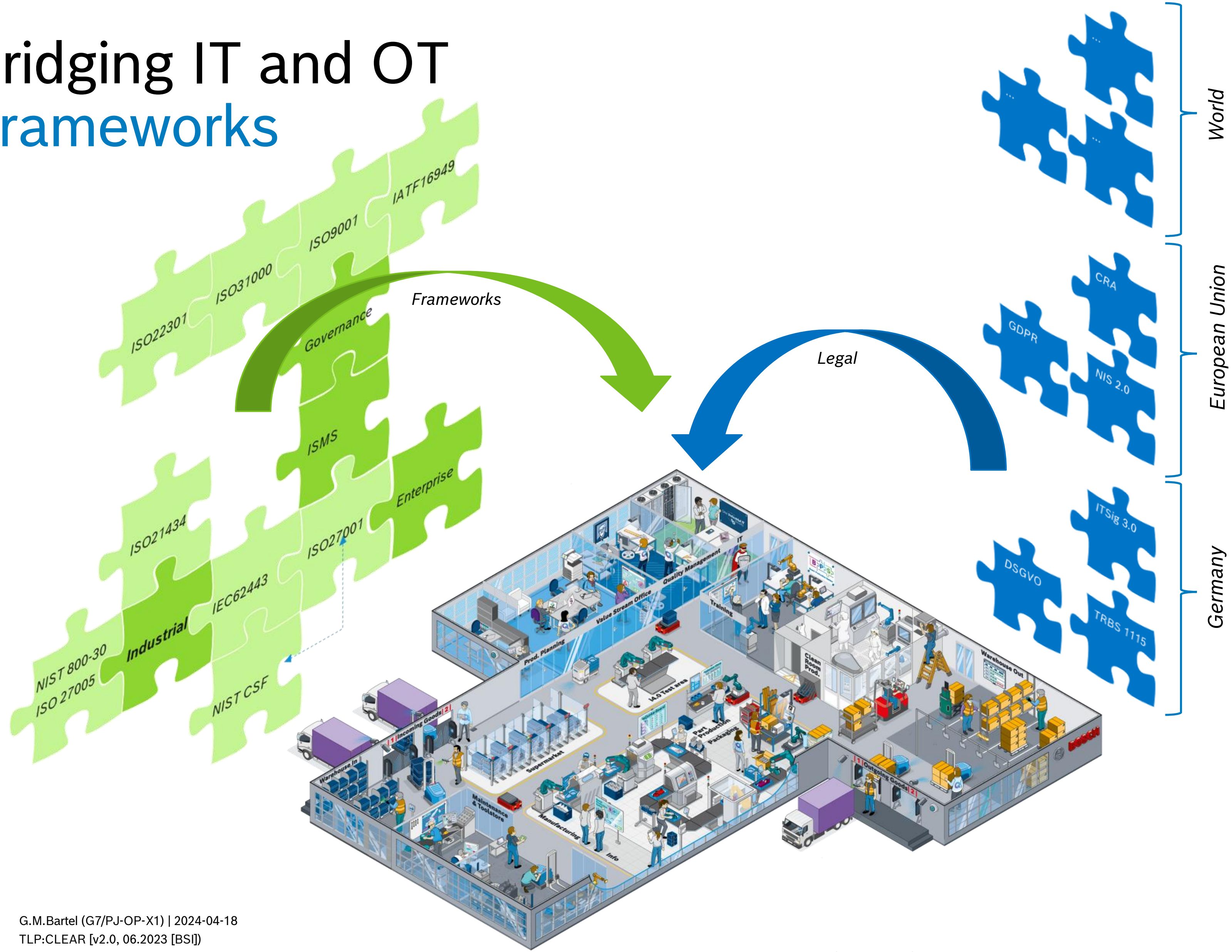
Challenges / opportunities

- Mostly centrally operated with standardized environments
- Generic setup with efficient and "up to date" functions
- On-prem / cloud convergence blurring operation of IT with 3rd parties
- Feature driven automated environment with high numbers of clients

Primary target
IT in general must comply with **integrity, availability, and confidentiality**, since information processed by the IT systems must be available to authorized users in an appropriate way.

[1] Operational technology (OT) is HW/SW that detects or causes a physical change, through the direct monitoring and/or control of industrial equipment, assets, processes and events [Gartner-ITG].

Bridging IT and OT
Frameworks



Industrial IT Security
Description

Definition
Industrial IT should address **IT security challenges** for operational technology owners (e.g., manufacturing, logistics, real estate) via **one framework**.

It must reflect the **primary target,** business model and **mission statements** of the affected units**.**

Mission Statement
Ensuring the availability, performance and integrity of all IT related **supporting assets** which contribute to the production capabilities serving as **primary asset**.

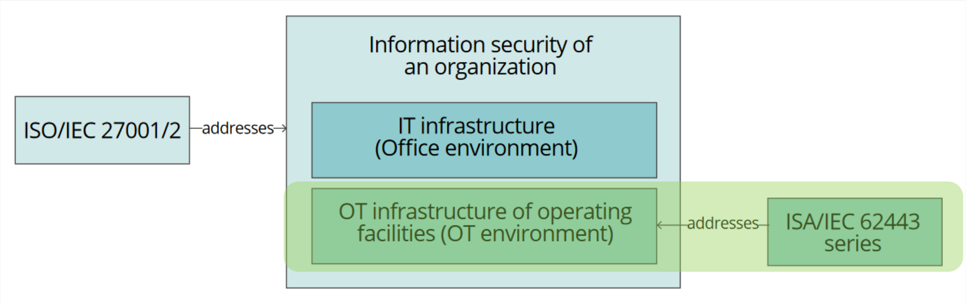
Defining and maintaining a **suitable industrial IT security framework** to ensure the competitiveness of the company.

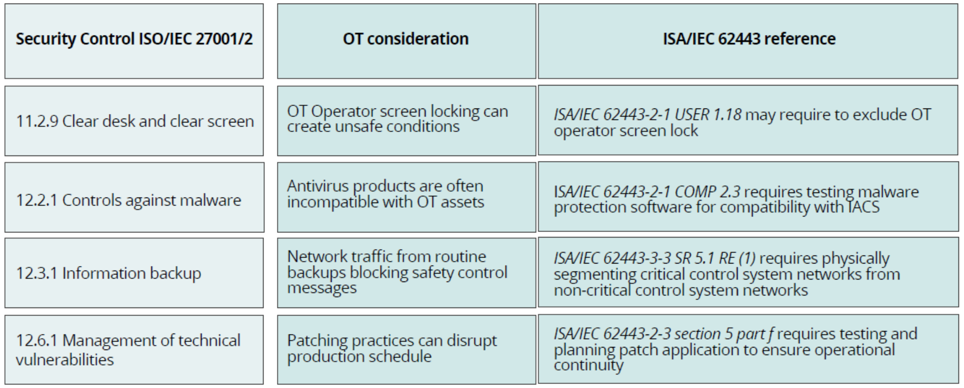
Challenges

- Decentralized operation & responsibilities
- OEE and cost driven operation
- Heterogenic & proprietary environment
- High amount of legacy IT systems
- IT/OT convergence
- Enabled and available personnel
- Legislative influences (e.g., NIS 2.0)

Bridging IT and OT
ISMS (ISO 27001/2) and IEC 62443

**ISAGCA, Applying ISO/IEC 27001/2 and ISA/IEC 62443 Series for OT Environments, 07.2021*


Information security of an organization
ISO/IEC 27001/2
addresses
IT infrastructure (Office environment)
OT infrastructure of operating facilities (OT environment)
addresses
ISA/IEC 62443 series

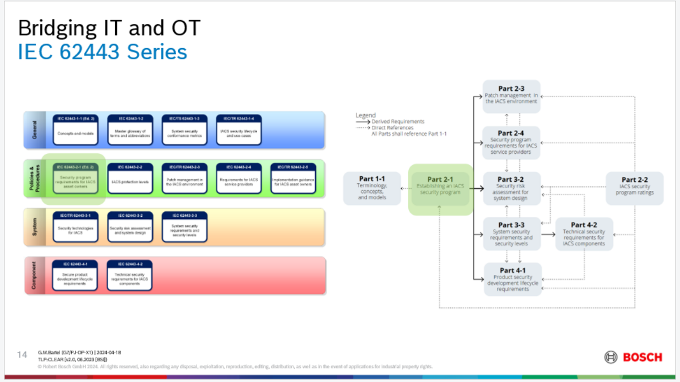


Security Control ISO/IEC 27001/2	OT consideration	ISA/IEC 62443 reference
11.2.9 Clear desk and clear screen	OT Operator screen locking can create unsafe conditions	*ISA/IEC 62443-2-1 USER 1.18* may require to exclude OT operator screen lock
12.2.1 Controls against malware	Antivirus products are often incompatible with OT assets	*ISA/IEC 62443-2-1 COMP 2.3* requires testing malware protection software for compatibility with IACS
12.3.1 Information backup	Network traffic from routine backups blocking safety control messages	*ISA/IEC 62443-3-3 SR 5.1 RE (1)* requires physically segmenting critical control system networks from non-critical control system networks
12.6.1 Management of technical vulnerabilities	Patching practices can disrupt production schedule	*ISA/IEC 62443-2-3 section 5 part f* requires testing and planning patch application to ensure operational continuity

- ISA/IEC 62443 series addresses **specific needs of OT**[1)] infrastructures and complements the ISMS
- It helps an organization to **maintain conformance** with ISO/IEC 27001 through:
  - common approaches wherever feasible,
  - while highlighting differences in IT vs. OT approach where needed
- ISO/IEC 27001/2 and the ISA/IEC 62443 series address two **complementary parts** of an overall OT cybersecurity approach.
- Considering the combination of the ISO/IEC 27001/2 controls[2)] and 62443-2-1 requirements **does not mean that all of them must be applied.**

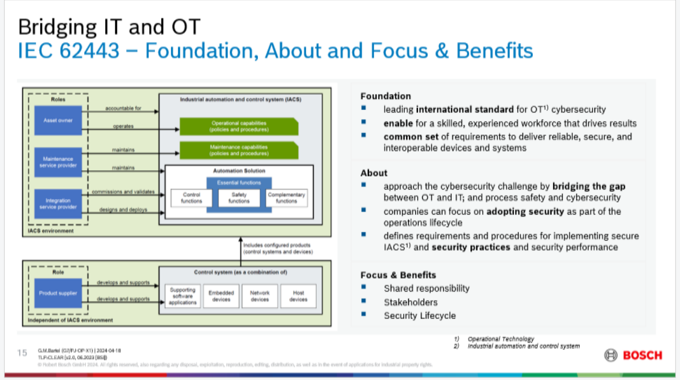
[1)] Operational technology (OT) is HW/SW that detects or causes a physical change, through the direct monitoring and/or control of industrial equipment, assets, processes and events [Gartner-ITG].
[2)] A control is a "measure that is modifying risk", [ISO27000]

Bridging IT and OT
ISMS (ISO 27001/2) and IEC 62443



Bridging IT and OT
IEC 62443 Series

General
IEC 62443-1-1 (Ed. 2)
Concepts and models
IEC 62443-1-2
Master glossary of terms and abbreviations
IEC/TS 62443-1-3
System security conformance metrics
IEC/TR 62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
IEC 62443-2-1 (Ed. 2)
Security program requirements for IACS asset owners
IEC 62443-2-2
IACS protection levels
IEC/TR 62443-2-3
Patch management in the IACS environment
IEC 62443-2-4
Requirements for IACS service providers
IEC/TR 62443-2-5
Implementation guidance for IACS asset owners
System
IEC/TR 62443-3-1
Security technologies for IACS
IEC 62443-3-2
Security risk assessment and system design
IEC 62443-3-3
System security requirements and security levels
Component
IEC 62443-4-1
Secure product development lifecycle requirements
IEC 62443-4-2
Technical security requirements for IACS components
Legend
Derived Requirements
Direct References
All Parts shall reference Part 1-1
Part 1-1
Terminology, concepts, and models
Part 2-1
Establishing an IACS security program
Part 2-3
Patch management in the IACS environment
Part 2-4
Security program requirements for IACS service providers
Part 3-2
Security risk assessment for system design
Part 3-3
System security requirements and security levels
Part 4-1
Product security development lifecycle requirements
Part 4-2
Technical security requirements for IACS components
Part 2-2
IACS security program ratings



Bridging IT and OT
IEC 62443 – Foundation, About and Focus & Benefits

Roles
Asset owner
Maintenance service provider
Integration service provider
accountable for
operates
maintains
maintains
commissions and validates
designs and deploys
Industrial automation and control system (IACS)
Operational capabilities (policies and procedures)
Maintenance capabilities (policies and procedures)
Automation Solution
Essential functions
Control functions
Safety functions
Complementary functions
IACS environment
Includes configured products (control systems and devices)
Role
Product supplier
develops and supports
develops and supports
Control system (as a combination of)
Supporting software applications
Embedded devices
Network devices
Host devices
Independent of IACS environment

Foundation

- leading **international standard** for OT[1] cybersecurity
- **enable** for a skilled, experienced workforce that drives results
- **common set** of requirements to deliver reliable, secure, and interoperable devices and systems

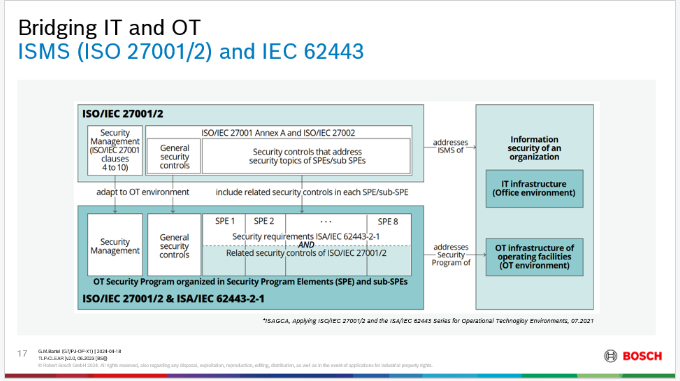
About

- approach the cybersecurity challenge by **bridging the gap** between OT and IT; and process safety and cybersecurity
- companies can focus on **adopting security** as part of the operations lifecycle
- defines requirements and procedures for implementing secure IACS[1] and **security practices** and security performance

Focus & Benefits

- Shared responsibility
- Stakeholders
- Security Lifecycle

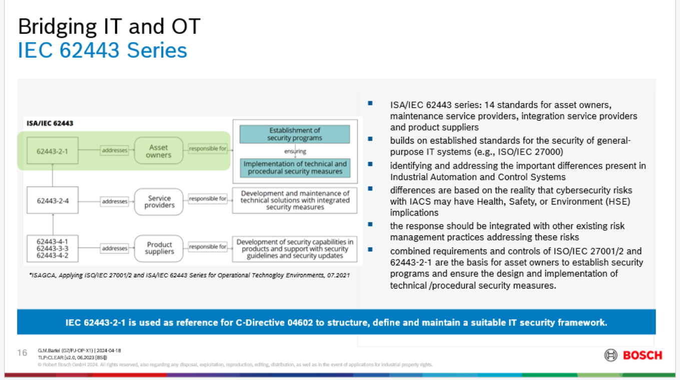
1) Operational Technology
2) Industrial automation and control system



Bridging IT and OT
ISMS (ISO 27001/2) and IEC 62443

ISO/IEC 27001/2
Security Management (ISO/IEC 27001 clauses 4 to 10)
ISO/IEC 27001 Annex A and ISO/IEC 27002
General security controls
Security controls that address security topics of SPEs/sub SPEs
adapt to OT environment
include related security controls in each SPE/sub-SPE
Security Management
General security controls
SPE 1
SPE 2
. . .
SPE 8
Security requirements ISA/IEC 62443-2-1
AND
Related security controls of ISO/IEC 27001/2
OT Security Program organized in Security Program Elements (SPE) and sub-SPEs
ISO/IEC 27001/2 & ISA/IEC 62443-2-1
addresses ISMS of
addresses Security Program of
Information security of an organization
IT infrastructure (Office environment)
OT infrastructure of operating facilities (OT environment)

**ISAGCA, Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technogloy Environments, 07.2021*



Bridging IT and OT
IEC 62443 Series

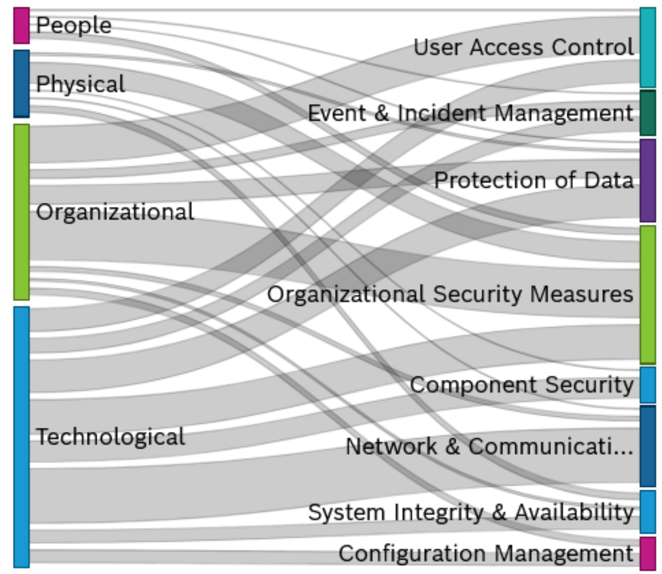
ISA/IEC 62443
62443-2-1
addresses
Asset owners
responsible for
Establishment of security programs
ensuring
Implementation of technical and procedural security measures
62443-2-4
addresses
Service providers
responsible for
Development and maintenance of technical solutions with integrated security measures
62443-4-1
62443-3-3
62443-4-2
addresses
Product suppliers
responsible for
Development of security capabilities in products and support with security guidelines and security updates

**ISAGCA, Applying ISO/IEC 27001/2 and ISA/IEC 62443 Series for Operational Technogloy Environments, 07.2021*

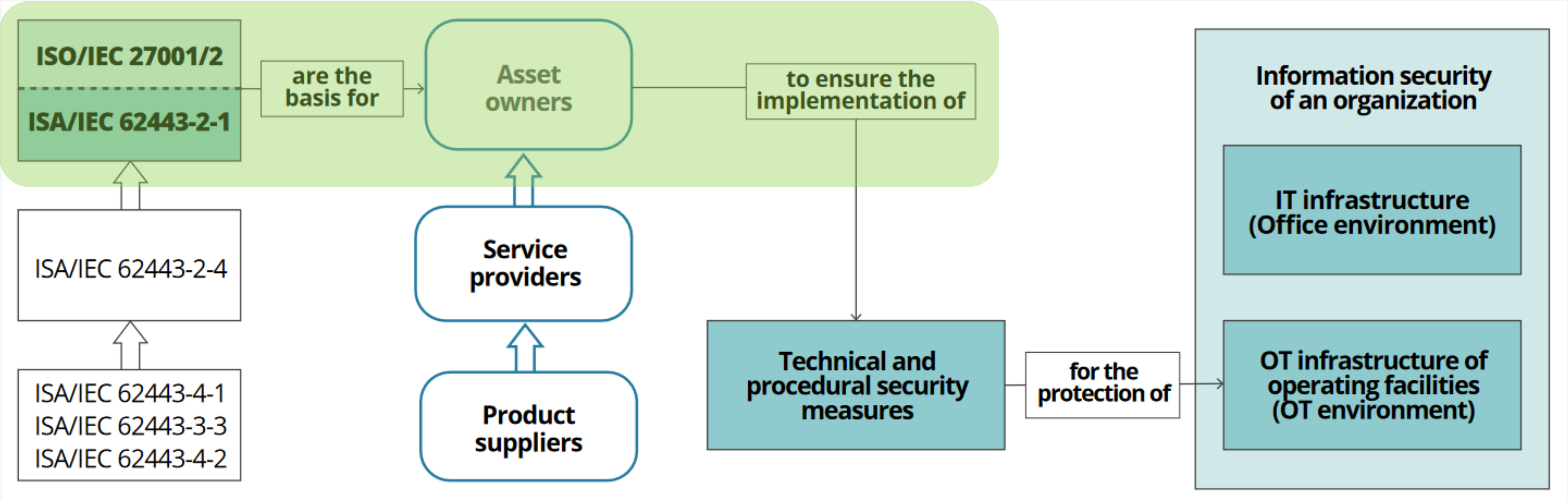
- ISA/IEC 62443 series: 14 standards for asset owners, maintenance service providers, integration service providers and product suppliers
- builds on established standards for the security of general-purpose IT systems (e.g., ISO/IEC 27000)
- identifying and addressing the important differences present in Industrial Automation and Control Systems
- differences are based on the reality that cybersecurity risks with IACS may have Health, Safety, or Environment (HSE) implications
- the response should be integrated with other existing risk management practices addressing these risks
- combined requirements and controls of ISO/IEC 27001/2 and 62443-2-1 are the basis for asset owners to establish security programs and ensure the design and implementation of technical /procedural security measures.

IEC 62443-2-1 is used as reference for C-Directive 04602 to structure, define and maintain a suitable IT security framework.

ISO 27002:2022 & IEC62443-2-1 type relations

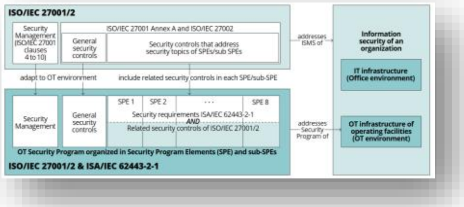


Bridging IT and OT
ISMS (ISO 27001/2) and IEC 62443

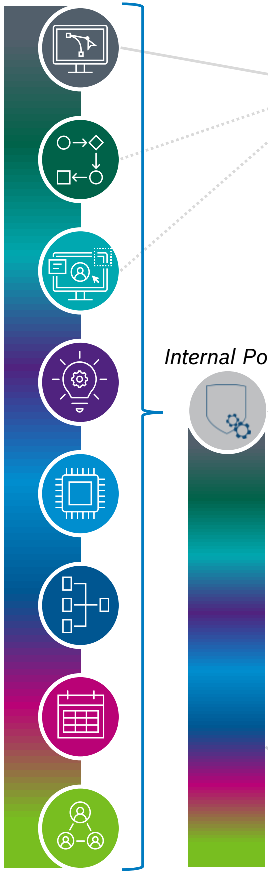

ISO/IEC 27001/2
ISA/IEC 62443-2-1
are the basis for
Asset owners
to ensure the implementation of
ISA/IEC 62443-2-4
Service providers
ISA/IEC 62443-4-1
ISA/IEC 62443-3-3
ISA/IEC 62443-4-2
Product suppliers
Technical and procedural security measures
for the protection of
Information security of an organization
IT infrastructure (Office environment)
OT infrastructure of operating facilities (OT environment)

**ISAGCA, Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technogloy Environments, 07.2021*

Bridging IT and OT
Approach

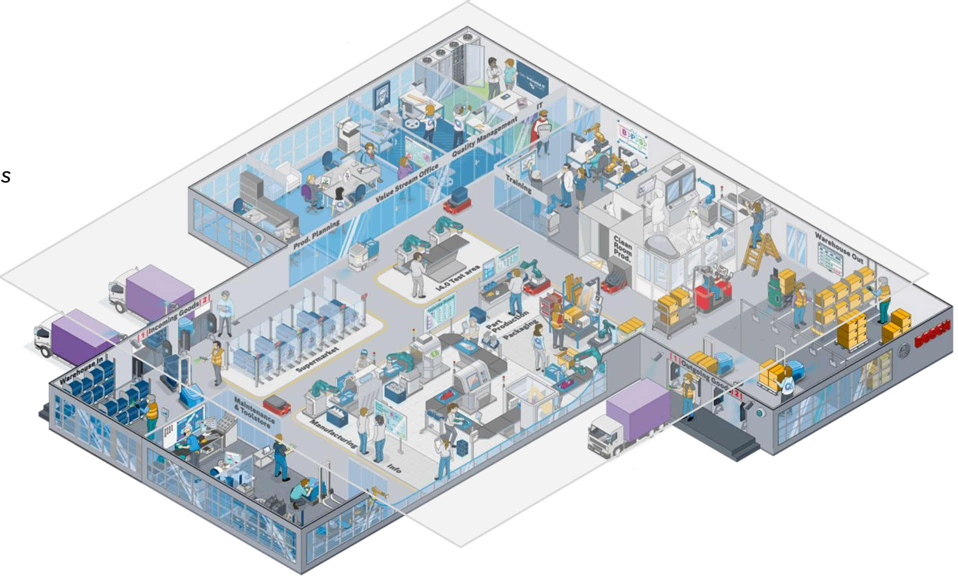

ISO/IEC 27001/2
Security Management (ISO/IEC 27001 clauses 4 to 10)
ISO/IEC 27001 Annex A and ISO/IEC 27002
General security controls
Security controls that address security topics of SPEs/sub SPEs
addresses ISMS of
Information security of an organization
IT infrastructure (Office environment)
adapt to OT environment
include related security controls in each SPE/sub-SPE
Security Management
General security controls
SPE 1
SPE 2
...
SPE 8
Security requirements ISA/IEC 62443-2-1
AND
Related security controls of ISO/IEC 27001/2
addresses Security Program of
OT infrastructure of operating facilities (OT environment)
OT Security Program organized in Security Program Elements (SPE) and sub-SPEs
ISO/IEC 27001/2 & ISA/IEC 62443-2-1

IEC 62443-2-1



SPE Categories

Security Program (SP)



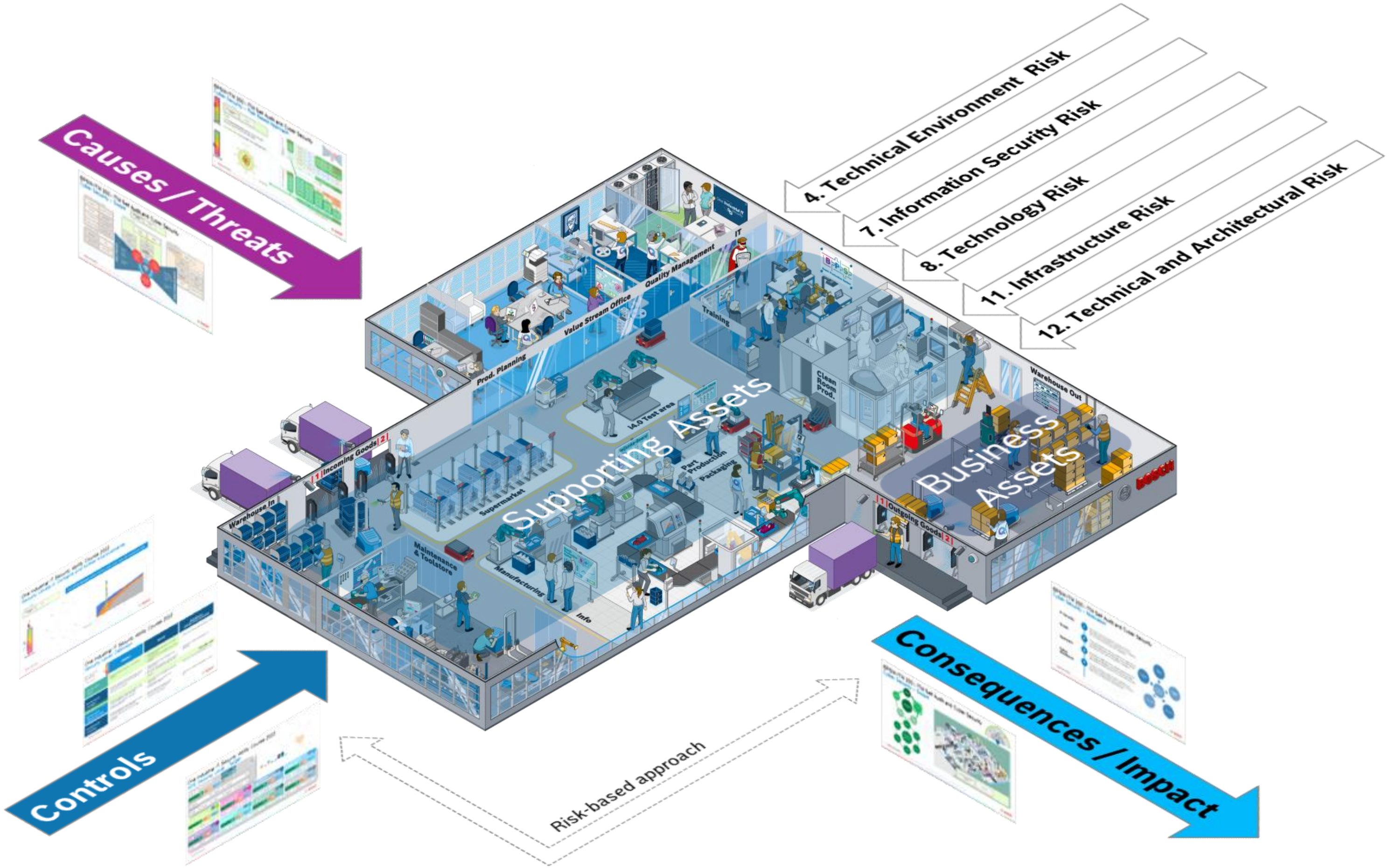
e.g., **SPE NET 1.1** *“ Segmentation and communications policies for interconnections between IACS network segments and non-IACS network segments are defined, enforced and updated.”*

1. **Select x out of 8** SPE categories (e.g., ORG, CM) deemed to contribute to preventive, detective and/or corrective actions.
2. Choose certain **SPEs** per **SPE category** to be implemented as **Security Program** due to their effectiveness and applicability (total: **x out of 89)**
3. Specify SPEs into different stages, e.g., **Level 0 to 4,** to allow heterogenous, realistic and measurable protection levels within industrial IT.
4. For each SPE **security levels** are defined as target **(e.g., domains)**. Such are then **aggregated** via its category to an overall score to be achieved.

**SP: Security Program*
SPE: Security Program Element
SL: Security Level

BOSCH

Bridging IT and OT
Field of Action



Entities and Locations
Risk Management Value Proposition

Description
Process and understand **IT related impulses** regarding negative changes and influences ahead of time via **standardized methods** to plan actions accordingly.

Motivation
- **Protect the company** (people, information, property, entrepreneurial success) and secure the foundation of your growth
- **Enable strategic decisions** and strengthen the trust in your company and community you operate

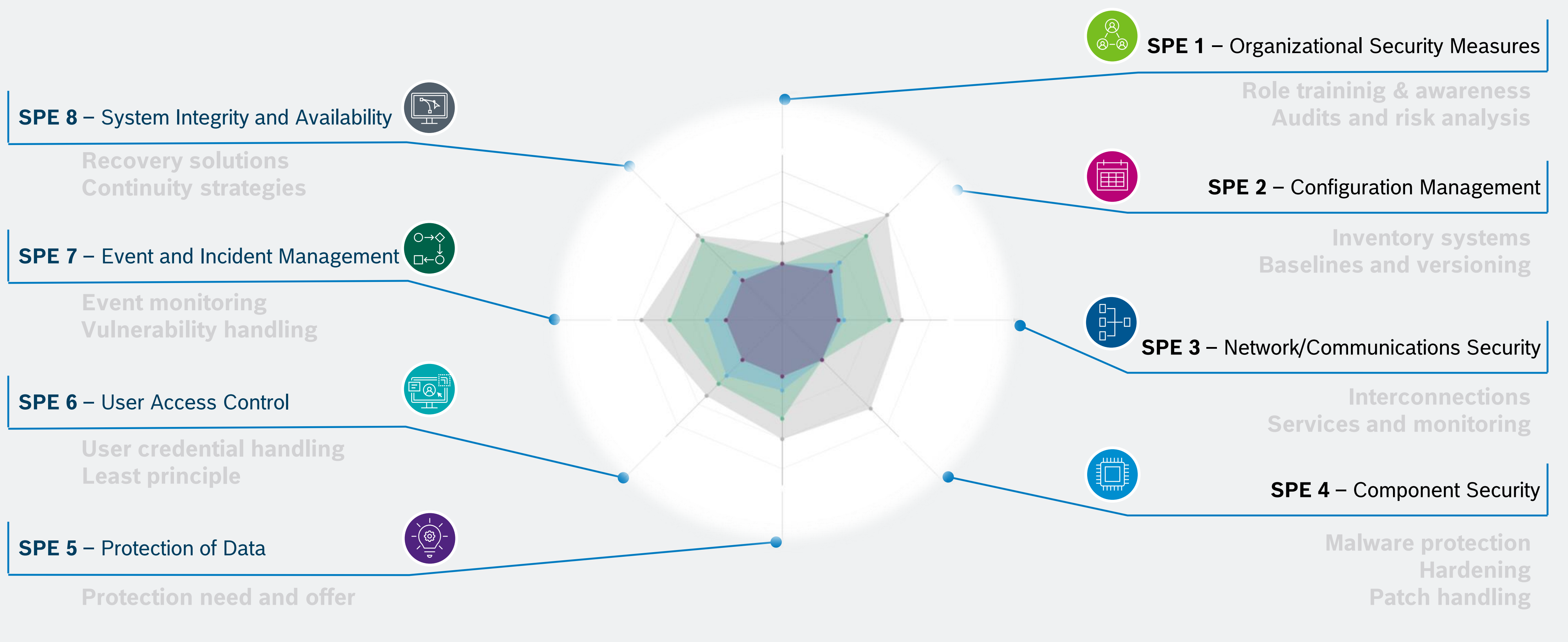
Approach
- Identify variety of local influencing factors
- Reduce risks with appropriate measures
- Take risks consciously

Apply **recognized frameworks** and methods for risk assessment by user friendly application by:
- **Decentralization** (you know your environment best)
- **Subsidiarity** (minimal standards acc. to your needs)
- **Governance** (leverage existing control regulations)

Monitor risks by transparency, analysis and documentation to capture IT related issues for industrial domain holistically addresses also legal obligations.

BOSCH

Bridging IT and OT
Field of Action (Examples)



SPE 1 – Organizational Security Measures

Role traininig & awareness
Audits and risk analysis

SPE 2 – Configuration Management

Inventory systems
Baselines and versioning

SPE 3 – Network/Communications Security

Interconnections
Services and monitoring

SPE 4 – Component Security

Malware protection
Hardening
Patch handling

SPE 5 – Protection of Data

Protection need and offer

SPE 6 – User Access Control

User credential handling
Least principle

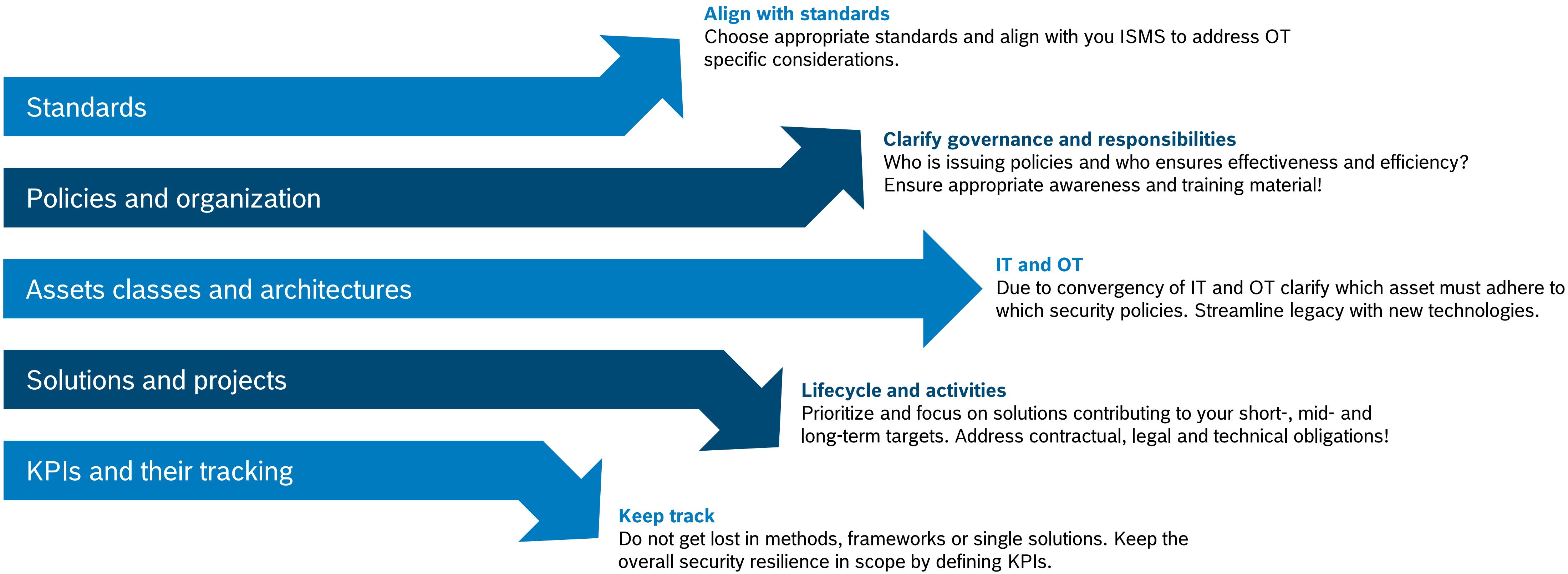
SPE 7 – Event and Incident Management

Event monitoring
Vulnerability handling

SPE 8 – System Integrity and Availability

Recovery solutions
Continuity strategies

Bridging IT and OT
Wrap Up



Standards

Policies and organization

Assets classes and architectures

Solutions and projects

KPIs and their tracking

Align with standards
Choose appropriate standards and align with you ISMS to address OT specific considerations.

Clarify governance and responsibilities
Who is issuing policies and who ensures effectiveness and efficiency? Ensure appropriate awareness and training material!

IT and OT
Due to convergency of IT and OT clarify which asset must adhere to which security policies. Streamline legacy with new technologies.

Lifecycle and activities
Prioritize and focus on solutions contributing to your short-, mid- and long-term targets. Address contractual, legal and technical obligations!

Keep track
Do not get lost in methods, frameworks or single solutions. Keep the overall security resilience in scope by defining KPIs.

One Industrial IT Security

Thank You!

G.M.Bartel, G7/PJ-OP-X1

BOSCH